Collaboration Endpoints

Revised: March 1, 2018

A variety of endpoints can be used in a Cisco Collaboration deployment. These endpoints range from gateways that support ordinary analog phones in an IP environment to an extensive set of native IP phones offering a range of capabilities.

When deploying endpoints, you need to consider several factors, including authentication, upgrades, signaling protocol, Quality of Service (QoS), and so forth. The collaboration system must be designed appropriately to accommodate these factors.

This chapter summarizes various types of collaboration endpoints and covers design and deployment considerations including high availability and capacity planning. The collaboration endpoints covered in this chapter can be categorized into the following major types:

The sections listed above provide information about each endpoint type, including deployment considerations. That information is followed by a discussion related to high availability, capacity planning, and design considerations for effectively deploying endpoints.

Use this chapter to understand the range of available endpoint types and the high-level design considerations that go along with their deployment.

What's New in This Chapter

Table 8-1 lists the topics that are new in this chapter or that have changed significantly from previous releases of this document.

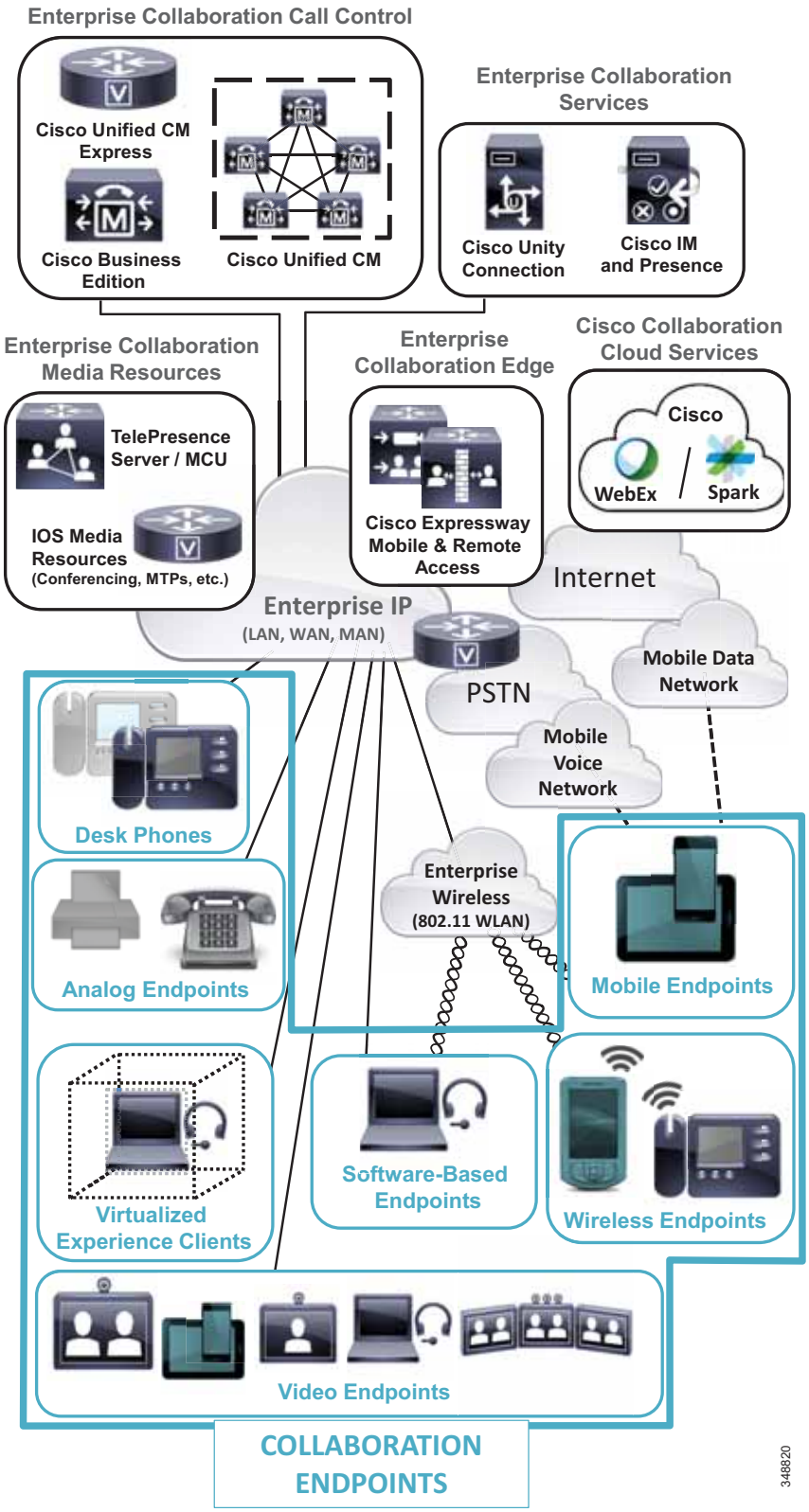
Table 8-1 New or Changed Information Since the Previous Release of This Document

New or Revised Topic	Described in:	Revision Date
Apple Push Notification service (APNs) for Cisco Jabber and Cisco Spark Apple iOS clients	Deployment Considerations for Mobile Endpoints and Clients, page 8-38	March 1, 2018
OAuth 2.0 with Refresh Token for Cisco Jabber	General Deployment Considerations for Software-Based Endpoints, page 8-29 Deployment Considerations for Mobile Endpoints and Clients, page 8-38	March 1, 2018
Cisco Spark Room Series	Cisco Spark Room Series, page 8-17	March 1, 2018
Cisco IP Phone 8800 Series	Cisco IP Phone 8800 Series, page 8-9	March 1, 2018

Collaboration Endpoints Architecture

Just as there is a variety of endpoint types, as shown in Figure 8-1, there is also a variety of call control, collaboration services, and media resource options that must be considered when deploying collaboration endpoints. Collaboration endpoints rely on enterprise call control and/or cloud-based collaboration for voice and video calling services. Collaboration endpoints also leverage both enterprise on-premises and cloud-based collaboration services such as voice messaging, instant messaging, and presence. Further, these endpoints gain key supplementary services from enterprise media resources such as video and voice conferencing, transcoding, and music on hold.

Figure 8-1 Cisco Collaboration Endpoints Architecture



While there are multiple options when deploying collaboration call control for voice and video services, each call control platform provides endpoint registration, call setup and routing services, and access to provisioned media resources. The high-level call control interactions between endpoints and the enterprise Cisco Unified Communications Manager is described in the following sub-section.

Cisco Unified Communications Manager (Unified CM) Call Control

Call signaling in Cisco Unified Communications Manager (Unified CM), Cisco Business Edition, and Cisco Unified Communications Manager Express (Unified CME) distinguishes between line-side signaling and trunk-side signaling. Whereas trunk-side signaling is used for connecting the entire call processing cluster or router to other servers and gateways, the line side is used for connecting endpoint devices to the call processing platform. The two interfaces are distinct in the services they offer, with the line side offering a rich set of user-oriented features.

Session Initiation Protocol (SIP) and Skinny Client Control Protocol (SCCP) are the two main line-side signaling protocols supported by Cisco call processing platforms. All Cisco endpoints support either or both of these protocols. The set of features supported in both protocols is roughly equivalent, and the choice of which protocol to use is essentially a personal preference in a deployment. However, SIP is the protocol of choice for support of all new features and Cisco endpoints.

Cisco endpoints must be configured with several operating parameters before they can be used to make or receive calls or to run applications. This configuration must be performed in advance on the call processing server or router. Once configured, the call processing platform generates a configuration file for the endpoint to use, and it stores that file on a Trivial File Transfer Protocol (TFTP) server. The endpoints themselves go through a boot-up sequence when powered on. They retrieve this configuration file before they register with the appropriate server, and then they are ready to be used. The endpoints execute the following steps as part of the boot-up sequence:

1. When connected to the access switch, if the endpoint is not plugged in to a power source, it attempts to obtain power from the switch (Power over Ethernet). Wireless and mobile endpoints are not connected to the enterprise network via Ethernet and therefore always derive power from a battery or power outlet.
2. Once power is obtained, if device security is enabled, the endpoint presents its credentials to the security server or network authentication infrastructure.
3. If it is allowed to use the network, the endpoint obtains its network parameters such as IP address, Domain Name Service (DNS) servers, gateway address, and so forth, either through static provisioning in the endpoint or through Dynamic Host Control Protocol (DHCP).
4. The endpoint also obtains a TFTP server address either through static provisioning or through DHCP options.
5. The endpoint then uses the TFTP server address to obtain its configuration files that, among other parameters, details the call processing server(s) or router(s) that the endpoint may associate and register with, the directory numbers that the endpoint must support, and so forth.
6. The endpoint registers with the call processing platform and is available for use.

To confirm which endpoints support registration to Cisco Unified CM, refer to the endpoint data sheets listed in various other sections of this chapter.

Collaboration Endpoint Section 508 Conformance

Regardless of the call control platform you choose, when selecting endpoints and designing your Cisco Collaboration network you should strive to make the telephony features more accessible to users with disabilities, in conformance with Section 255 of the Telecommunications Act and U.S. Section 508.

Observe the following basic design guidelines when configuring your Cisco Unified Communications network to conform to Section 508:

- Enable Quality of Service (QoS) and call admission control on the network to ensure optimal quality of voice and video so that enterprise communications are as clear and precise as possible.
- Configure only the G.711 codec for phones that will be connected to a terminal teletype (TTY) device or a Telephone Device for the Deaf (TDD). Although low bit-rate codecs such as G.729 are acceptable for audio transmissions, they do not work well for TTY/TDD devices if they have an error rate higher than 1% Total Character Error Rate (TCER).
- Configure TTY/TDD devices for G.711 across the WAN, if necessary.
- Enable (turn ON) Echo Cancellation for optimal performance.
- Voice Activity Detection (VAD) does not appear to have an effect on the quality of the TTY/TDD connection, so it may be disabled or enabled. However, Cisco recommends leaving VAD (also known as silence suppression) disabled on Unified CM call control and using the **no vad** command on H.323 and Cisco IOS SIP dial-peers.
- Configure the appropriate *regions* and *device pools* in Unified CM to ensure that the TTY/TDD devices always use G.711 codecs.
- Connect the TTY/TDD to the Cisco Unified Communications network in either of the following ways:
  - Direct connection (Recommended method)

    Plug a TTY/TDD with an RJ-11 analog line option directly into a Cisco FXS port. Any Cisco voice gateway with an FXS port will work. Cisco recommends this method of connection.
  - Acoustic coupling

    Place the IP phone handset into a coupling device on the TTY/TDD. Acoustic coupling is less reliable than an RJ-11 connection because the coupling device is generally more susceptible to transmission errors caused by ambient room noise and other factors.
- If stutter dial tone for audible message waiting indication (AMWI) is required, use an analog phone in conjunction with an FXS port on the Cisco VG Analog Gateways or Analog Telephony Adaptor (ATA). In addition, most Cisco IP Phones support stutter dial tone.
- When you deploy immersive Cisco TelePresence rooms, ensure that ample room is provided to accommodate and provide for unimpeded movement of wheel chairs and other assistive conveyances.

Analog Endpoints

An analog gateway typically is used to connect analog devices such as fax machines, modems, telecommunications device for the deaf (TDD)/teletypewriter (TTY), and analog phones, to the VoIP network so that the analog signal can be packetized and transmitted over the IP network. Analog gateways also provide physical connectivity to the PSTN and other traditional telephony equipment such as PBXs and key systems. Analog gateways include Cisco IOS router-based analog interface or service modules as well as fixed-port standalone gateways. Generally analog gateways rely on Cisco

Unified CM, Cisco Business Edition, Unified CM Express, and even Survivable Remote Site Telephony (SRST) for call control, supplementary services, and in some cases interface registration and configuration. Call control protocols supported across Cisco analog gateways include SIP, H.323, SCCP, and Media Gateway Control Protocol (MGCP).

Standalone Analog Gateways

Cisco standalone analog gateways, including the Cisco Analog Telephony Adaptor (ATA) and Cisco VG Series Gateway, provide connectivity for analog devices such as fax machines, modems, TDD/TTY, paging systems, and analog phones, as well as one or more Ethernet ports for connecting to the IP network. Cisco standalone analog gateways support the FXS analog telephony interface port type only.

For more information on Cisco ATAs, refer to the data sheets and documentation for the ATA 190 Series at:

https://www.cisco.com/c/en/us/products/unified-communications/ata-190-series-analog-telephone-adapters/index.html

For more information on Cisco VG Series Gateways, refer to the data sheets and documentation at:

https://www.cisco.com/c/en/us/products/unified-communications/vg-series-gateways/index.html

Analog Interface Module

Cisco IOS router-based analog interface modules, including network modules (NMs) and voice interface cards (VICs), connect the PSTN and other legacy telephony equipment, including PBXs, analog telephones, fax machines, and key systems, to Cisco multiservice access routers such as the Cisco Integrated Services Router (ISR). Cisco IOS analog interface modules support a wide range of analog telephony interface port types, including FXS, FXO, T1/E1, E&M, and BRI.

Cisco IOS version support is critical for successful deployment of analog interface modules. For more information on Cisco IOS-based analog interface modules, including interface port type and Cisco IOS version support, refer to the data sheets and documentation listed at

https://www.cisco.com/c/en/us/products/collateral/routers/4000-series-integrated-services-routers-isr/datasheet-c78-733646.html

Deployment Considerations for Analog Endpoints

The following sections list important design considerations for deploying analog endpoints.

Analog Connection Types

The choice of analog connection type is typically dictated by the type of analog connection being made. For example, an FXS or E&M interface provides ring and dial tone for basic telephone handsets, while FXO interfaces are used for trunk or tie line connections to a PSTN or to an enterprise PBX. In all cases these interfaces indicate on-hook or off-hook status and the seizure of telephone lines.

With FXO and FXS analog connections there are two types of access signaling methods: loop start or ground start. The type of signaling used is ultimately determined by the type of service from the PSTN. Typically standard telephone land lines use loop start, but business telephone lines and trunks usually rely on ground start. A loop start line does not maintain any current on the circuit until it is in use, whereas a ground start line maintains some current on the line. The use of constant current on the ground

start line typically requires specialized equipment on the PSTN side, which typically makes these lines more expensive than loop start lines. However, with ground start lines, because a loss of current on the line is immediately detected on the far side of the analog connection, the gateway or PBX gets immediate indication regarding connects and disconnects, thus providing better control over the connection. In addition, a ground start trunk reduces the possibility of "glare," or the collision of simultaneous incoming and outgoing calls on the line.

E&M interfaces support different signaling methods, including wink start and immediate start. Wink start is the most common form of E&M signaling, and it relies on a "wink" sequence (on-hook, off-hook, on-hook) indication from the far end in response to an initial off-hook indication at the call origination side before digits can be sent over the interface. In contrast, immediate start signaling relies on a brief pause rather than a response from the far end after the initial off-hook indication before digits are sent.

The analog interface type used in a particular deployment will ultimately be dictated by the interface supported by the PSTN provider or by the equipment deployed in the case of internal analog connections. In all cases, you should use the supported method of signaling for the analog connection type that provides the most visibility and control of the line. For example, with FXS or FXO, ground start is preferred over loop start because of the end-to-end line current which, when broken, can be detected immediately. Likewise, with E&M, wink start is preferred over immediate start because of the positive indication from the far end that digits can be sent.

For additional information on Cisco analog telephony signaling, refer to the documentation available at

https://www.cisco.com/c/en/us/tech/voice/telephony-signaling/index.html

Paging Systems

In some IP telephony deployments, the enterprise IP PBX is integrated with a paging system that allows users to call an extension on the system that forwards the audio broadcast to overhead loudspeakers. These overhead paging systems are useful in workshops, parking lots, and open plant areas where a called party is not near a telephone handset. Integration to these paging systems is done using an analog interface module port.

Cisco analog gateways and interface modules support all traditional analog port types used for paging system integration, including FXO, FXS, and E&M. When integrating with overhead paging systems, ensure that the appropriate analog interface module port type, signaling, and configuration are used as required by the paging system being integrated. The port type, signaling, and configuration will ultimately be dictated by the paging system.

An example of an E&M interface integration to an overhead paging system is available at

https://www.cisco.com/c/en/us/support/docs/voice/analog-signaling-e-m-did-fxs-fxo/27627-e-mpaging.html

Quality of Service

When configuring network-level quality of service (QoS), Cisco analog gateways such as the standalone Cisco VG Series and the Cisco IOS-based analog interface modules can be trusted and their packet markings honored. By default they mark their voice media and signaling packets with appropriate Layer 3 values (voice media as DSCP 46 or PHB EF; call signaling as DSCP 24 or PHB CS3), which match Cisco QoS recommendations for appropriate voice media and signaling marking, so as to ensure end-to-end voice quality on a converged network.

Desk Phones

The Cisco IP Phone portfolio includes the following family of desk phones:

Cisco Unified IP Phone 7900 Series

The Cisco Unified IP Phone 7900 Series of endpoints consists of several models and feature sets. In general, all phones in the Unified IP Phone 7900 Series provide the same basic set of enterprise IP telephony features such as call hold, call transfer, call forwarding, and so forth. However, the 7900 Series also provides features and functions well beyond the traditional enterprise IP telephony feature set, including support for IP-based phone services to enable presence, messaging, mobility, security, and other network-based applications and services. The Cisco Unified IP 7900 Series supports both SCCP and SIP signaling protocols for registering and communicating with the Cisco call processing platforms.

In some cases additional line keys can be added to Unified IP Phone 7900 Series devices by physically attaching a key expansion module such the Cisco Unified IP Phone Expansion Module 7916. This gives administrative assistants and other users the ability to answer and/or determine the status of a number of lines beyond the current line capability of their desk phone. Some Unified IP Phone 7900 Series models are capable of supporting up to two Cisco Unified IP Phone Expansion Modules, but the use of an external power adaptor may be required.

Note When two Expansion Modules are used with a single phone, the second module must be the same model as the first one.

For more information about the Cisco Unified IP Phone 7900 Series, refer to the data sheets and documentation at

https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-7900-series/index.html

Cisco IP Phone 7800 Series

The Cisco IP Phone 7800 Series of endpoints includes a number of models ranging from the single-line Cisco IP Phone 7811 to the larger, more advanced 16-line Cisco IP Phone 7861. These phone models have LCD displays, built-in speakerphone, and PC ports. In general, all of the phones in the IP Phone 7800 Series provide enterprise IP telephony features such as hold, call transfer, call forwarding, and so forth. The Cisco IP 7800 Series supports SIP signaling protocol for registering and communicating with the Cisco call processing platforms.

Note Starting with Cisco IP Phone 7800 Series firmware version 11.0(1)and with Cisco Expressway X8.7 and later versions, the 7800 Series officially supports Cisco Expressway as an alternative to VPN access. Expressway provides enterprise firewall traversal for 7800 Series voice calls.

For more information about the Cisco IP Phone 7800 Series, refer to the data sheets and product documentation available at

https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-7800-series/index.html

Cisco IP Phone 8800 Series

The Cisco IP Phone 8800 Series of endpoints delivers a highly secure and comprehensive feature set with support for wideband audio. For example, the new Cisco IP Conference Phone 8832 provides dynamic, detailed sound with low distortion and low-frequency clarity. Both wired and Digital Equipment Cordless Telephony (DECT) wireless extension microphones are available for 360-degree coverage in conference room deployments. In addition, the IP Phone 8800 Series personal endpoints, from the 8811 to the 8865, provide a range of features. Some models in this series, such as the 8845, 8851, 8861, and 8865, provide support for Bluetooth and Intelligent Proximity for Mobile Voice as well as smartphone or tablet charging via on-board USB ports. New Key Expansion Modules (KEM) have been introduced for the 8800 Series that provide dual LCD support to maximize the viewing area and improve the user experience. A new audio KEM and video KEM have been introduced. Also, the 8845 and 8865 provide HD 720p built-in video camera support. In general, all of the phones in the IP Phone 8800 Series provide an identical set of enterprise IP telephony features such as call hold, call transfer, call forwarding, and so forth. These endpoints support SIP signaling protocol for registering and communicating with the Cisco call processing platforms.

Note Starting with Cisco IP Phone 8800 Series firmware version 11.0(1) and with Cisco Expressway X8.7 and later versions, the 8800 Series phone models officially support Cisco Expressway as an alternative to VPN access. Expressway provides enterprise firewall traversal for 8800 Series voice and video calls.

Note Starting with Cisco IP Phone 8800 Series firmware version 11.5, the 8800 Series phone models support Enhanced Line Mode, which allows for the assignment of programmable lines or features such as speed dials to all 10 line keys. Prior to this firmware enhancement, only 5 programmable line keys could be used on the phone. In addition, firmware version 12.0 adds support to Enhanced Line Mode for call park, extension mobility cross cluster, group pickup, and hunt groups.

For more information about the Cisco IP Phone 8800 Series, refer to the data sheets and other documentation at

https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/index.html

Cisco Unified SIP Phone 3900 Series

The Cisco Unified SIP Phone 3900 Series provides cost-effective, entry-level endpoints that support a single line and provide a basic set of enterprise IP telephony capabilities and basic supplementary features such as mute, call hold, and call transfer. The Cisco Unified SIP Phone 3900 Series has a two-line liquid crystal display (LCD) screen and a half-duplex or full-duplex speakerphone (depending on the model). The Cisco Unified SIP Phone 3900 Series supports the SIP signaling protocols for registering and communicating with Cisco call processing platforms.

Note The Cisco Unified SIP Phone 3900 Series does not support features such as CTI (for Jabber phone control), speed dials, or Built-in Bridge for Silent Monitoring and Recording. The Cisco IP Phone 7800 Series or 8800 Series are recommended for environments requiring the full set of enterprise grade IP telephony features.

For more information about the Cisco Unified SIP Phone 3900 Series, refer to the data sheets and documentation at

https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-sip-phone-3900-series/index.html

Cisco DX Series

The DX Series of endpoints delivers integrated Unified Communications, high-definition (HD) video, and collaboration applications and services. The Cisco DX Series endpoints provide wideband audio and HD video for enterprise-class communications with integrated 7 to 23 inch (model dependent) multi-touch LCD display and front-facing camera. These devices run secure Android operating system and provide access to a variety of integrated collaboration and communication applications including calendaring, corporate directory searches, email, Jabber IM and presence, visual voicemail, and WebEx conferencing as well as AnyConnect VPN for secure network attachment. In addition, as an open Android platform, these devices are capable of accessing the Google Play store for access to many third-party applications that enable additional features and functionality. These endpoints also provide a variety of external interfaces for attaching accessories, including: HDMI for connecting external devices such as a laptop or external display (model dependent); USB for keyboard, mouse, or wired headset attachments; and Bluetooth for connecting a wireless headset, keyboard, and/or mouse, or for leveraging Intelligent Proximity for Mobile Voice.

The DX Series endpoints support SIP signaling protocol for registering and communicating with Cisco call processing platforms. Cisco Unified Communications Manager is required to deploy and support the DX Series.

Note Starting with Cisco DX Series firmware version 10.2.4, the DX Series supports Cisco Expressway as an alternative to VPN access. Expressway provides enterprise firewall traversal for DX Series voice and video, as well as the built-in Jabber IM application.

For more information about the Cisco DX Series, refer to the data sheets and documentation at

https://www.cisco.com/c/en/us/products/collaboration-endpoints/desktop-collaboration-experience-dx600-series/index.html

Deployment Considerations for Cisco Desk Phones

The following sections list important design considerations when deploying Cisco desk phones.

Firmware Upgrades

Most commonly, and by default, IP phones upgrade their images using HTTP, which uses Port 6970, from TFTP services integrated into one or more of the call processing platforms. When HTTP is not available, IP phones use TFTP, which is a UDP-based protocol from the same TFTP services. With this arrangement, all the phones obtain their images directly from these TFTP services. This method works well for a relatively small number of phones or if all of the phones are located in a single campus region that has a LAN environment with essentially unlimited bandwidth.

For larger deployments that use centralized call processing, upgrading phones in branch offices that are connected to the central data center by low-speed WAN links, can require a large amount of data traffic over the WAN. The same set of files will have to traverse the WAN multiple times, once for each phone. Transferring this amount of data is not only wasteful of the WAN bandwidth but can also take a long time as each data transfer competes with the others for bandwidth. Moreover, due to the nature of TFTP protocol, some phones might be forced to abort their upgrades and fall back to the existing version of the code.

Note During the upgrade, the Cisco IP Phones 7800, 8800, and DX Series stay in service, unlike the 7900 Series phones. The 7800, 8800, and DX Series phones download and store the new firmware in their memory while still maintaining their active status, and they reboot with the new firmware only after a successful download.

Two methods are available to alleviate problems created by the need to upgrade phones over the WAN. One method is to use a local TFTP server just for the upgrades. The administrator can place a TFTP server in branch offices (particularly in branches that have a larger number of phones, or whose WAN link is not speedy or robust), and can configure the phones in those offices to use that particular TFTP server just for new firmware. With this change, phones will retrieve new firmware locally. This upgrade method would require the administrator to pre-load the phone firmware on the TFTP server in the branch and manually configure the TFTP server address in the **load server** parameter in the affected phone configurations. Note that the branch router may be used as a TFTP server.

The second method to upgrade phones without using the WAN resources excessively is to use the Peer File Sharing (PFS) feature. With this feature, typically only one phone of each model in the branch downloads each new firmware file from the central TFTP server. Once the phone downloads the firmware file, it distributes that file to other phones in the branch. This method avoids the manual loading and configuration required for the load server method.

The PFS feature works when the same phone models in the same branch subnet arrange themselves in a hierarchy (chain) when asked to upgrade. They do this by exchanging messages between themselves and selecting the "root" phone that will actually perform the download. The root phone sends the firmware file to the second phone in the chain using a TCP connection; the second phone sends the firmware file to the third phone in the chain, and so on until all of the phones in the chain are upgraded. Note that the root phone may be different for different files that make up the complete phone firmware.

Power Over Ethernet

Deploying desk phones with inline power-capable switches enables these endpoints to derive power over the Ethernet network connection, thus eliminating the need for an external power supply as well as a wall power outlet. Inline power-capable switches with uninterruptible power supplies (UPS) ensures that power over Ethernet (PoE) capable IP desk phones continue to receive power during power failure situations. Provided the rest of the telephony network is available during these periods of power failure, then IP phones should be able to continue making and receiving calls.

Depending on the type of desk phone and the PoE standard supported by both the desk phone and the inline power-capable switch, in some cases the power budget of the inline powered switch port may be exceeded. This typically occurs when attaching key extension modules or other power consuming attachments such as USB cameras. In these situations, the phone may need to be powered using a wall outlet and external power supply or else the switch providing the power may need to be upgraded.

Note In addition to using the inline power from the access switch or local wall power, a Cisco Unified IP Phone can also be supplied power by a Cisco Unified IP Phone power injector. The Cisco Unified IP Phone power injector connects Cisco Unified IP Phones to Cisco switches that do not support inline power or to non-Cisco switches. The Cisco Unified IP Phone power injector is compatible with most Cisco Unified IP Phones. It has two 10/100/1000 Base-T Ethernet ports. One Ethernet port connects to the switch access port and the other connects to the Cisco Unified IP Phone.

Quality of Service

When configuring network-level quality of service (QoS), Cisco desk phones such as the Cisco Unified IP Phone 7900, 8800, and DX Series can be trusted and their packet markings honored. By default these endpoints mark their voice media and signaling packets with appropriate Layer 3 values (voice media as DSCP 46 or PHB EF; call signaling as DSCP 24 or PHB CS3), which match Cisco QoS recommendations for appropriate voice media and signaling marking, to ensure end-to-end voice quality on a converged network. While many Cisco desk phones support the attachment of a desktop computer, Cisco desk phones are capable of separating the voice and data traffic, placing voice traffic onto the voice VLAN and data traffic from the desktop onto the data VLAN. This enables the network to extend trust to the phone but not to the PC port of the phone. However, for multipurpose devices such as the Cisco DX Series endpoints, which are capable of generating both voice and data traffic without an attached desktop computer, both voice and data traffic will traverse the same VLAN. In these cases, whether the device is attached to the voice or data VLAN, extending trust to these devices might not be advisable. Instead, re-marking the traffic based on port and protocol will ensure that all traffic is appropriately marked regardless of the VLAN it traverses.

In deployment where there are concerns about the potential volume of data traffic generated by multipurpose devices such as the Cisco DX Series and the possibility of adversely impacting real-time voice and video traffic, these devices should be deployed in the data VLAN or in a separate VLAN. This will alleviate concerns about impacting call quality of voice and video-only devices. Further, with packet re-marking based on ports and protocols, priority treatment can still be provided within the VLAN to real-time traffic generated by these multipurpose devices.

Note While many Cisco desk phones support Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED), they do so only for VLAN and Power over Ethernet negotiation. Cisco Unified IP Phones do not honor DSCP and CoS markings provided by LLDP-MED.

SRST and Enhanced SRST

When deploying Cisco desk phones in branch locations separated from a centralized call processing platform by a low-speed or unreliable WAN link, it is important to consider local call processing redundancy. By leveraging Survivable Remote Site Telephony (SRST) or Enhanced SRST on a Cisco IOS router in each branch location, basic IP telephony services can be maintained for the desk phones when connectivity to the centralized call processing platform is lost. However, the set of available user-facing features is much smaller when a device is registered to SRST than when the phone is registered to Unified CM.

Secure Remote Enterprise Attachment

Cisco desk phones can be securely connected to the enterprise network from remote locations using VPN or VPN-less solutions.

In the case of VPN-based connectivity, desk phones can be located behind a VPN router that creates a secure VPN tunnel to the Cisco Adaptive Security Appliance (ASA) or other VPN head-end concentrator at the enterprise edge. Alternatively, some phone models support a native built-in VPN client that provides VPN connectivity within the phone itself for voice traffic (media and signaling) of the device, but not for the PC or data traffic. In this case the phone creates a secure VPN tunnel to the Cisco ASA within the enterprise. The native built-in VPN client is supported only on certain phone models, including the Cisco Unified IP Phone 7945, 7965, and 7975, as well as the 8800 Series phones. For more information on built-in VPN on Cisco Unified IP Phones, refer to the latest version of the *Security Guide for Cisco Unified Communications Manager*, available at

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

Note The 7800 Series does not support built-in VPN. The 7800 Series does support Expressway Mobile and Remote Access starting with firmware version 11.0(1) and with Expressway X8.7 and later versions.

Cisco IP Phone 7800 Series, IP Phone 8800 Series, and DX Series endpoints are able to leverage mobile and remote access functionality of the Cisco Expressway solution. This firewall traversal solution relies on TLS reverse proxy connectivity to the enterprise, as provided by the Cisco Expressway-E and Expressway-C servers for registration to Unified CM call control for voice and video calling. For more information about mobile and remote access capabilities of the Cisco Expressway solution, refer to the solution information and product documentation available at

https://www.cisco.com/c/en/us/products/unified-communications/expressway-series/index.html

Intelligent Proximity

Intelligent Proximity refers to features that leverage proximity-based connections between Cisco hardware endpoints and mobile devices.

Intelligent Proximity for Mobile Voice capabilities available on the Cisco DX Series and select 8800 Series endpoints rely on the use of Bluetooth pairing between the DX or 8800 endpoint and a cellular or smart phone.

Bluetooth paired mobile devices are able to invoke two features:

- Hands-free audio, providing the ability to send audio of a cellular terminated call through the DX Series, 8845, 8851, 8861, or 8865 IP endpoint speaker or handset. Audio play-out of the cellular terminated call can be moved back and forth between the DX, 8845, 8851, 8861, or 8865 and the mobile device. In addition, because the Bluetooth paired mobile device appears on the 8845, 8851, 8865, or DX Series endpoints as another line, cellular calls on the Bluetooth paired mobile device can be initiated using the DX or 8800 IP endpoint.
- Mobile contact and call history sharing, providing the ability to share mobile device contact and call history sharing with the DX Series, 8845, 8851, 8861, or 8865 endpoints.

Because Intelligent Proximity for Mobile Voice relies on Bluetooth pairing, there is no requirement to run an application or client on the mobile device. All communication and interaction occurs over the standard-based Bluetooth interfaces.

The Intelligent Proximity for Mobile Voice feature set on the DX Series endpoints and the 8845, 8851, 8861, and 8865 IP phones is compatible with the Unified Mobility feature set, including single number reach (SNR), remote destination and desk phone pickup, two-stage enterprise dialing, and mobile voicemail avoidance. In the case of the 8845, 8851, 8861, and 8865 IP phones, Intelligent Proximity for Mobile Voice is compatible with Cisco Jabber mobile clients. When a Jabber client running on a mobile device is paired with the 8845, 8851, 8861, or 8865 IP phone, the audio portion of a Jabber call may be played out using the 8845, 8851, 8861, or 8865 handset or speaker while the video portion of the call continues to play on the Jabber mobile client. In the case of DX Series endpoints, Intelligent Proximity for Mobile Voice functionality is limited exclusively to the cellular line of Bluetooth paired mobile devices running Jabber.

The Intelligent Proximity for Mobile Voice feature set on the DX Series and select 8800 Series endpoints requires firmware version 10.1.1 or later.

Note Starting with Cisco IP Phone 8800 Series firmware version 11.0(1), the 8845, 8851, 8861, and 8865 phones support Cisco Unified CM Application Dial Rules that allow for dialing imported smartphone contacts over a Cisco VoIP network.

For more information about Intelligent Proximity for Mobile Voice, refer to the product documentation for the Cisco DX Series and 8800 Series endpoints as well as the information at

https://www.cisco.com/c/en/us/products/collaboration-endpoints/intelligent-proximity.html

Video Endpoints

Cisco video endpoints provide IP video telephony features and functions similar to IP voice telephony, enabling users to make point to point and point to multi-point video calls. Cisco offers the following video-capable endpoints:

- Cisco Jabber software-based desktop clients such as Cisco Jabber for Windows
- Cisco Unified IP Phones 8800 Series (8845 or 8865) with built-in camera
- Cisco DX Series with built-in camera
- Cisco TelePresence System EX, MX, SX, and IX Series
- Cisco Spark Room Kit Series

Cisco video endpoints deliver high-quality video for all user types and environments within any organization. Cisco video endpoints are classified into families based on the features they support, hardware screen size, and environment where the endpoint is deployed. This section categorizes the Cisco video endpoint families into personal, multipurpose, and immersive endpoints groups.

Personal Video Endpoints

Personal video endpoints provide a high-quality, face-to-face video calling experience for personal workspaces.

Cisco Jabber Desktop Video

Cisco Jabber software-based desktop clients, such as Cisco Jabber for Windows, are able to send and receive video when running on a desktop computer with an integrated or USB attached camera. These video-capable software-based endpoints register and communicate with Unified CM call control and operate as a SIP single-line voice and video enabled phone. These endpoints support the primary and backup registration redundancy mechanisms as provided by Unified CM. The Cisco Jabber software-based endpoint processes video on the computer where it is installed. The quality of the decoding and encoding depends on the availability of CPU and memory resources on that computer.

For additional information on Cisco Jabber desktop clients, refer to Software-Based Endpoints, page 8-22.

For more information about the video capabilities of Cisco Jabber for Windows, refer to the data sheet and product documentation available at

https://www.cisco.com/c/en/us/products/unified-communications/jabber-windows/index.html

Cisco IP Phone 8800 Series

Some models in this series, specifically the 8845 and 8865, provide support for HD 720p with an integrated video camera. The main difference between the 8845 and the 8865 is that the 8865 also provides support for smartphone or tablet charging via on-board USB ports. Also, the 8865 provides support for up to three Key Expansion Modules. In general, the 8845 and 8865 provide an integrated video experience along with enterprise IP telephony features such as call hold, call transfer, call forwarding, and so forth. These endpoints support SIP signaling protocol for registering and communicating with the Cisco call processing platforms.

For more information about the Cisco IP Phone 8800 Series, refer to the data sheets and documentation at

https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/index.html

Cisco DX Series

The Cisco DX Series endpoints are capable of transmitting video by means of the built-in front-facing camera. These endpoints are capable of receiving and displaying video natively on their screens with a variety of video resolutions and frame rates. The video capabilities of these phones can be enabled and disabled or tuned as desired from the Cisco call control platform configuration pages.

These devices register and communicate with Unified CM using SIP signaling protocol.

For more information about the Cisco DX Series video capabilities, refer to the data sheets and product documentation available at

https://www.cisco.com/c/en/us/products/collaboration-endpoints/desktop-collaboration-experience-dx600-series/index.html

Cisco TelePresence System EX90

The Cisco TelePresence System EX90 video endpoint takes the personal desktop solution to a next level of experience with support for full high definition (HD) video calls and added features such as content sharing. The EX90 has a wide screen with support for the multisite feature that provides the ability to add participants into a Cisco TelePresence call and dual display for content sharing.

The Cisco TelePresence System EX90 video endpoint registers and communicates with Unified CM by means of the SIP signaling protocol.

For more information about the Cisco TelePresence EX90 video endpoint, refer to the data sheets and product documentation available at

https://www.cisco.com/c/en/us/products/collaboration-endpoints/telepresence-system-ex-series/index.html

Multipurpose Video Endpoints

Multipurpose video endpoints enable any size meeting room to become a telepresence room by providing high quality point-to-point or multipoint video collaboration with content sharing.

Cisco TelePresence System MX Series

The MX Series of Cisco TelePresence endpoints provide highly integrated collaboration room systems that are classified as multipurpose room systems. These video endpoints are simple to use and easy to install, providing video calling and content sharing during presentations. They are cost-effective endpoints that can transform any room or existing meeting space into a multipurpose conference room providing full high definition (HD) video calling. There are four variants of the MX Series:

- MX800 single or dual 70-inch screen integrated TelePresence system
- MX700 is a dual 55-inch screen integrated TelePresence system
- MX300 G2 is a 55-inch screen integrated TelePresence system
- MX200 G2 is a 42-inch screen integrated TelePresence system

These endpoints register to Unified CM using the SIP signaling protocol.

For more information about the Cisco TelePresence System MX Series of video endpoints, refer to the data sheets and product documentation available at

https://www.cisco.com/c/en/us/products/collaboration-endpoints/telepresence-mx-series/index.html

Cisco TelePresence SX Series

The Cisco TelePresence SX Series endpoints are flexible integrators that can turn any flat-panel display into a powerful Cisco TelePresence system. The SX Series video endpoints are designed for HD video and multiparty conferencing, with the flexibility to accommodate various room sizes. This is an ideal solution for small to mid-size business and enterprises looking for a cost effective TelePresence-enabled conference room solution. The SX series video endpoints provide the following options:

- SX10 is an all-in-one system codec with integrated camera.
- SX20 is a codec with one of three camera options, and it supports the multisite features, providing the ability to add up to three more participants in a Cisco TelePresence call.
- SX80 is a codec that includes integrator packages supporting different camera and touch panel options.

These endpoints register to Unified CM using the SIP signaling protocol.

For more information about the Cisco TelePresence SX Series video endpoint, refer to the data sheets and product documentation available at

https://www.cisco.com/c/en/us/products/collaboration-endpoints/telepresence-quick-set-series/index.html

Cisco Spark Room Series

The Cisco Spark Room Series endpoints include both highly integrated collaboration room systems that can transform any room or existing meeting space into a multipurpose conference room as well as flexible integrators that can turn any flat-panel display into a powerful Cisco TelePresence system. The Cisco Spark Room Series video endpoints are designed for 4K ultra HD video and screen sharing and multi-party conferencing, with the flexibility to accommodate various room sizes.

There are four variants of the Cisco Spark Room Series:

- Cisco Spark Room Kit is an all-in-one system codec with integrated camera
- Cisco Spark Room Kit Plus is a quad camera system with separate codec
- Cisco Spark Room 55 is a 55-inch screen integrated TelePresence system
- Cisco Spark Room 70 is a single or dual 70-inch screen integrated TelePresence system

These endpoints register to Cisco Unified CM using the SIP signaling protocol or to the Cisco Collaboration Cloud using HTTPS.

For more information about the Cisco Spark Room Series video endpoints, refer to the data sheets and product documentation available at

https://www.cisco.com/c/en/us/products/collaboration-endpoints/spark-room-series/index.html

Immersive Video Endpoints

Immersive video endpoints enable the best possible in-person telepresence video collaboration experience, where attendees across multiple locations feel as though they are in the same room.

Cisco TelePresence IX5000 Series

The Cisco TelePresence IX5000 Series raises the standard for "in-person" collaboration with an industry first H.265 three-screen TelePresence system. This immersive system is not only easy to use but also very easy to set up. The system comes in two variants: the single-row 6-seat IX5000 system and the dual-row 18-seat IX5200 system. These systems are capable of delivering three simultaneous high-definition (1080p, 60 fps) video streams and two content sharing streams (1080p, 30 fps). These endpoints register to Unified CM using the SIP signaling protocol.

For more information about the Cisco TelePresence IX5000 Series immersive video systems, refer to the data sheets and product documentation available at

https://www.cisco.com/c/en/us/products/collaboration-endpoints/ix5000-series/index.html

General Deployment Considerations for Video Endpoints

The following sections list important design considerations for deploying video endpoints.

Quality of Service

When configuring network-level quality of service (QoS), Cisco video endpoints (including Cisco DX Series and Cisco TelePresence System devices) generally mark traffic at Layer 3 according to Cisco general QoS guidelines related to voice and video packet marking (voice media as DSCP 46 or PHB EF; desktop video media as DSCP 34 or PHB AF41; telepresence video media as DSCP 32 or PHB CS4; call signaling as DSCP 24 or PHB CS3), and therefore these devices can be trusted. In the case of personal desktop video endpoints, including Cisco DX Series devices, both voice and video media packets are marked as DSCP 34 or PHB AF41 to preserve lip synchronization during a video call.

While proper network QoS configuration is essential even when the endpoint marking is trusted, Cisco recommends ensuring that sufficient bandwidth is provisioned on the network and then using network-based policing and rate limiting to ensure that all endpoints do not consume more network bandwidth than they should. Software-based video-capable endpoints do present challenges when they do not or cannot mark traffic appropriately. In these situations, typical guidance is to re-mark media and signaling traffic within the network from best-effort to appropriate and recommended values (voice media as DSCP 46 or PHB EF; desktop video and voice media for video calls as DSCP 34 or PHB AF41; telepresence video media as DSCP 32 or PHB CS4; call signaling as DSCP 24 or PHB CS3) based on protocols and/or port numbers.

In the case of software-based Cisco Jabber for Windows, appropriate Layer 3 DSCP QoS marking can be applied to audio and video streams based on voice and video media source port numbers using Microsoft Windows group policies.

For more information about Cisco Jabber for Windows QoS with Microsoft Windows group policies, refer to the Quality of Service configuration information in the latest version of *On-Premises Deployment for Cisco Jabber*, available at

https://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html

Note While some Cisco video-capable endpoints support Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED), they do so only for VLAN and Power over Ethernet negotiation. Cisco video endpoints do not honor DSCP and CoS markings provided by LLDP-MED.

For more information on video endpoint network bandwidth consumption and QoS marking and classification, see the section on WAN Quality of Service (QoS), page 3-37.

Inter-VLAN Routing

When deploying video endpoints on networks with voice and data VLAN separation, it is important to consider software-based video-capable endpoints as well as hardware-based video endpoints that need to access resources. Because software-based endpoints running on a desktop computer are primarily attached to the data VLAN, inter-VLAN routing should be configured and allowed so that voice traffic from these endpoints on the data VLAN can reach endpoints on the voice VLAN. Likewise, if hardware-based video endpoints such as the Cisco TelePresence System endpoints need access to network resources such as directory or management services deployed on the data VLAN, inter-VLAN routing must be allowed.

SRST and Enhanced SRST

When deploying video endpoints in branch locations separated from a centralized call processing platform by a low-speed or unreliable WAN link, it is important to consider local call processing redundancy. By deploying SRST or Enhanced SRST on a Cisco IOS router in each branch location, basic IP telephony services can be maintained for most video endpoints when connectivity to the centralized call processing platform is lost. The set of available user-facing features is much smaller when a video endpoint is registered to SRST than when the application is registered to Unified CM. Specifically, video endpoint devices registered to SRST will be capable of making and receiving only voice calls (audio-only). SRST is not supported with the Cisco TelePresence System video endpoints. However, starting with Cisco IOS Release 15.3(3)M using phone load firmware 9.4.1 or later, Enhanced SRST supports making and receiving video calls with some video endpoints during WAN failure. For details on Enhanced SRST video support for various phone models, refer to the Cisco Unified IP Phone documentation available at

https://www.cisco.com/

Secure Remote Enterprise Attachment

Cisco video endpoints can be securely connected to the enterprise network from remote locations using VPN or VPN-less solutions.

In the case of VPN-based connectivity, all video endpoints can be located behind a VPN router that creates a secure VPN tunnel to the Cisco Adaptive Security Appliance (ASA) or other VPN head-end concentrator at the enterprise edge. In addition, the Cisco Unified IP Phone 8800 Series supports a native built-in VPN client, which provides VPN connectivity within the phone itself for voice and video traffic (media and signaling) without the need for a VPN router.

For VPN-less connectivity, Cisco TelePresence endpoints running TC firmware (EX, MX, C, and SX Series endpoints) as well as DX Series endpoints are able to leverage mobile and remote access functionality of the Cisco Expressway solution. This firewall traversal solution relies on TLS reverse proxy connectivity to the enterprise as provided by the Cisco Expressway-E and Expressway-C servers

for registration to Unified CM call control for voice and video calling. For additional information on mobile and remote access capabilities of the Cisco Expressway solution, refer to the solution information and product documentation available at

https://www.cisco.com/c/en/us/products/unified-communications/expressway-series/index.html

Intelligent Proximity

As previously mentioned, Intelligent Proximity refers to features that leverage proximity-based connections between Cisco hardware endpoints and mobile devices.

Intelligent Proximity for Mobile Voice capabilities available on the Cisco IP Phone 8800 Series or the Cisco DX Series rely on Bluetooth pairing between the DX endpoint and a cellular or smart phone, enabling hands-free audio and mobile contact and call history sharing.

For more information on Intelligent Proximity and Bluetooth pairing, see Intelligent Proximity, page 8-13.

Video Interoperability

Video interoperability is the audio and video support for point-to-point calls between Cisco TelePresence System video endpoints, other Cisco Collaboration video endpoints, and third-party video endpoints. Previously, video interoperability between different families of video endpoints was possible only with the insertion of a video component between endpoints, such as a video transcoder or a multipoint control unit (MCU).

Cisco Unified CM not only offers native video interoperability between different video endpoint family types, but also provides better video interoperability in general with H.264 codec negotiation in SIP and H.323 protocols and enable the endpoints to negotiate high definition (HD) resolutions when available. Video interoperability, however, is dependent on the endpoints to support the interoperation.

Video interoperability in Unified CM also enables Cisco TelePresence System video endpoints to communicate with non-video endpoints, provided that the installed firmware supports such interoperability. For further information, refer to the *Cisco TelePresence Interoperability Database*, available at

https://tp-tools-web01.cisco.com/start/

Additionally, Cisco Unified CM provides support for enhanced interoperability with call agents other than Unified CM. Through scripting, Unified CM supports the following features:

- SIP transparency — The ability to pass through known and unknown message components
- SIP normalization — Transformations on inbound and outbound SIP messages and content bodies

The primary motivation for video interoperability support is to facilitate the interaction of a diverse set of video endpoints without the need for deploying an expensive hardware-based DSP infrastructure that would otherwise be required. There are additional benefits that can be derived from the use of advanced conferencing and transcoding resources (for example, active presence where participants of multi-point conferences can see the active speaker); however, the desired feature set and video calling needs will dictate when and where those advanced resources would be required.

The following sections present general considerations and recommendations for the use of video interoperability:

- Video Interoperability Architecture, page 8-21
- Design Considerations for Video Interoperability, page 8-21

Video Interoperability Architecture

The video interoperability architecture includes the following elements:

- Video interoperability support available with Cisco Unified CM
- Two different video endpoint family types (Cisco TelePresence System video endpoints, other Cisco Collaboration video endpoints such as the Cisco DX80, or third-party endpoints) engaged in a video call

The following sections offer further information about the scope of the video interoperability support:

- Video Interoperability Test Cases, page 8-21
- Limitations of Video Interoperability, page 8-21

Video Interoperability Test Cases

In most cases a video endpoint that supports SIP or H.323 without using proprietary signaling would be able to interoperate with a Cisco Collaboration video endpoint that supports video interoperability. For specific information on the scope of the interoperability between common sets of deployed devices and general information about the testing that was conducted to validate these more common examples of interoperability, refer to the Cisco Collaboration Systems documentation available at

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/unified/communications/system/ucstart.html

Limitations of Video Interoperability

While video interoperability support attempts to enable any-to-any point-to-point video call interoperability, it is important to note that not all features of an individual video endpoint can be supported when interoperating with another endpoint. There are many reasons for this. For example, incompatibilities between different call control protocols could render a feature unavailable or offer a different representation of that feature. H.264 video media parameters can be represented differently in H.323 than in SIP, as another example. H.323 also does not have support for presence, but presence is quite commonly supported in SIP. Skinny Client Control Protocol (SCCP) does not have any notion of application sharing, which is commonly available in SIP and H.323 endpoint implementations. For instance, an SCCP user trying to share his/her PC screen would be hampered because Binary Floor Control Protocol (BFCP) and H.239 are not available with SCCP.

Design Considerations for Video Interoperability

The following areas should be considered when implementing the video interoperability capabilities of Unified CM:

- Guideline and Restrictions for Video Interoperability, page 8-22
- Quality of Service (QoS) and Call Admission Control Considerations for Video Interoperability, page 8-22

Guideline and Restrictions for Video Interoperability

The following guidelines and restrictions apply with regard to video interoperability in a Unified CM deployment:

- If H.323 or SCCP protocols are used in conjunction with video interoperability, Unified CM will support only a single H.264 payload and the packetization mode is treated as 0. An example side effect (but not the only one) of this circumstance is the fact that 1080p resolution is not available with these protocols because 1080p requires packetization mode 1.
- If multiple payloads are presented by an H.323 or SCCP endpoint engaged in a video interoperability call, Unified CM will use only the payload with the lowest codec profile. This, in turn, could result in less than the highest supported resolution being selected for the call.
- If a SIP endpoint omits the **level-asymmetry-allowed** parameter in the Session Description Protocol (SDP), Cisco products will assume that the endpoint can support asymmetric resolution transmission. Therefore, different receiving and sending video resolutions could be negotiated during a call.
- If a call is processed with video interoperability while Unified CM is performing protocol interworking with SIP and H.323, the H.323 video endpoint must honor the proposed dynamic payload number specified by the SIP side, which means that no re-negotiation to a different payload would be supported.
- Unified CM will not negotiate Real-Time Transport Control Protocol (RTCP) feedback if the video call invokes a media termination point (MTP) or transcoder.

Quality of Service (QoS) and Call Admission Control Considerations for Video Interoperability

There are no changes to the configuration of regions and locations in Unified CM as a result of video interoperability support. However, regions play a significant role in determining the resolution between groups of endpoints, and they can be used to maximize or minimize the resolution that these devices use when interoperating. The **Max Video Call Bit Rate** field in the regions settings is used to determine the amount of bandwidth and, thus, the resolution that endpoints are able to negotiate.

For further information about QoS and call admission control with native video interoperability, see the section on Call Admission Control Design Recommendations for Video Deployments, page 13-78.

Software-Based Endpoints

A software-based endpoint is an application installed on a client desktop computer that registers and communicates with Cisco call processing platforms for voice and video services. In addition, these endpoint software client applications may provide collaboration features and services such as messaging, presence, directory access, and conferencing. Software-based endpoint desktop client applications include Cisco IP Communicator and Cisco Jabber.

Cisco IP Communicator

Cisco IP Communicator is a Microsoft Windows-based application that provides enterprise IP phone functionality to desktop computers. This application provides enterprise-class IP voice calling for remote users, telecommuters, and other mobile users. Cisco IP Communicator supports both SCCP and SIP signaling protocols for registering and communicating with Cisco call processing platforms. For more information about Cisco IP Communicator, refer to the data sheets and product documentation at

https://www.cisco.com/c/en/us/products/collaboration-endpoints/ip-communicator/index.html

Cisco Jabber Desktop Clients

Cisco Jabber desktop clients enable integration of collaboration services, including audio, video, web collaboration, visual voicemail, and so forth, into a software-based desktop application. Cisco Jabber allows desktop application users to access a variety of communication and collaboration services as provided by back-end collaboration application servers such as Cisco Unified Communications Manager (Unified CM), Cisco IM and Presence, Cisco Unity Connection, Cisco WebEx, and Lightweight Directory Access Protocol (LDAP)-compliant directories. Cisco Jabber is able to leverage IM and presence capabilities provided by either on-premises Cisco IM and Presence or the Cisco WebEx Messenger cloud service.

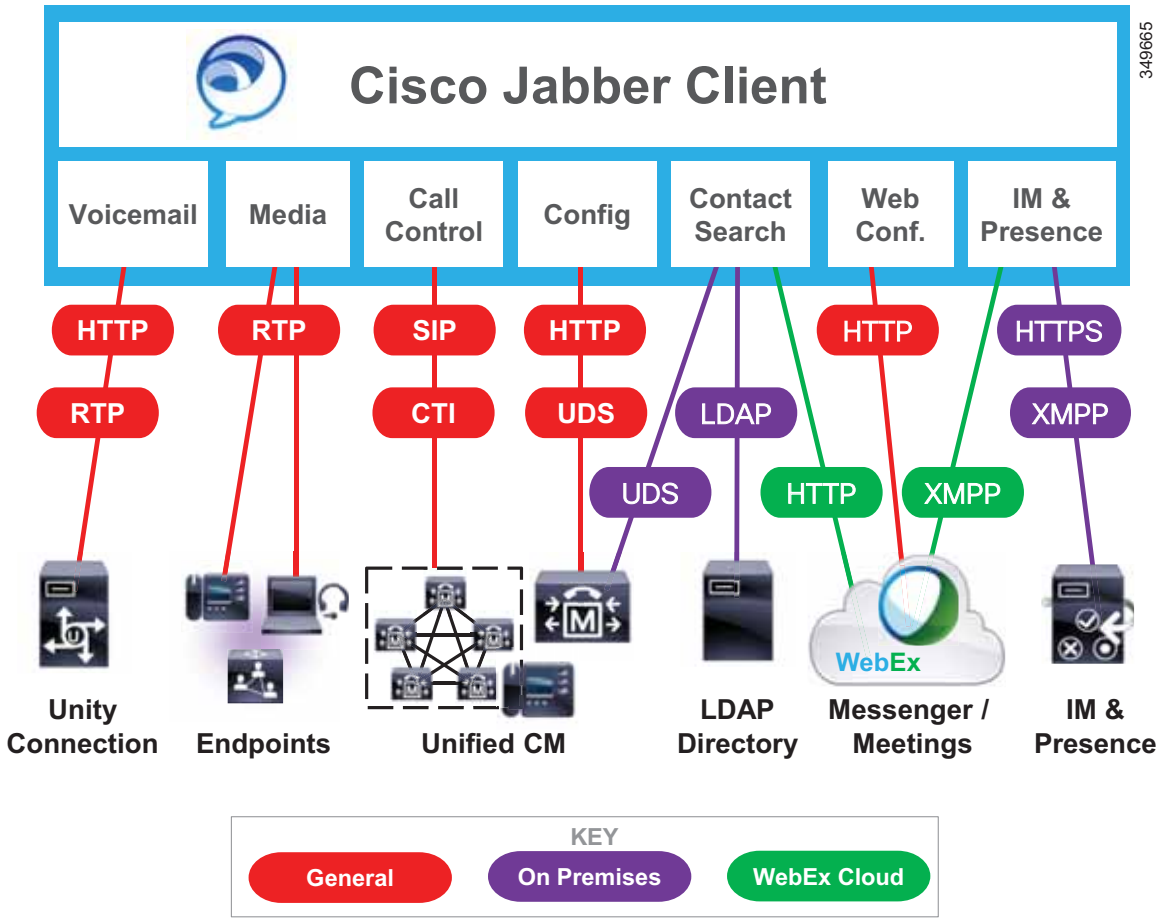
Cisco Jabber Desktop Client Architecture

Cisco Jabber for Windows and Cisco Jabber for Mac use a common set of services to provide various Cisco collaboration features, including instant messaging and presence, audio, video, web collaboration, visual voicemail, and so forth. This common set of services provides a simplified client interface and an abstraction layer that allows access to the following underlying communications services:

- SIP-based call control for voice and video softphone clients from Unified CM
- Deskphone call control and "Click to Call" services from the Unified CM CTI interface
- Voice and video media termination for softphone clients
- Instant messaging and presence services using XMPP, from either the Cisco IM and Presence Service or Cisco WebEx Messenger service. Cisco WebEx Meeting Center also offers hosted collaboration services such as online meetings and events.
- Viewing scheduled audio, video and web conferencing services
- Desktop sharing using either video desktop sharing (BFCP) or WebEx desktop sharing
- Visual voicemail services from Cisco Unity Connection using Internet Message Access Protocol (IMAP) or Representational State Transfer (REST)
- Contact management relying on Unified CM User Data Service (UDS), Microsoft Active Directory, or other supported LDAP directories; or in the case of cloud-based integrations, the WebEx Messenger service
- Microsoft Outlook Integration, which provides user availability status and messaging capabilities directly through the user interface of Microsoft Office applications such as Microsoft Outlook

The ability to communicate and abstract services and APIs, as shown in Figure 8-2, allows the Jabber Desktop Client to coordinate the management of protocols to these services and APIs, handle event notifications, and control the low-level connection logic for local system resources. Depending on the deployment type, some features might not be supported.

Figure 8-2 Cisco Jabber Desktop Client Architecture



Jabber Desktop Clients – Instant Messaging and Presence Services

Instant messaging and presence services for Jabber clients are provided through an XMPP interface. Cisco offers instant messaging and presence services with the following products:

- Cisco IM and Presence
- WebEx Messenger service

The choice between Cisco IM and Presence or WebEx Messenger service for instant messaging and presence services can depend on a number of factors. WebEx Messenger service deployments use a cloud-based service that is accessible from the Internet. On-premises deployments based on Cisco IM and Presence provide the administrator with direct control over their IM and presence platform and also allow presence federation using SIP/SIMPLE to other presence services.

For information on the full set of features supported by each IM and Presence platform, refer to the following documentation:

- Cisco IM and Presence

  https://www.cisco.com/c/en/us/products/unified-communications/unified-presence/index.html

- WebEx Messenger service

  https://www.cisco.com/c/en/us/products/unified-communications/webex-messenger/index.html

Jabber Desktop Clients – Call Control

Cisco Jabber Desktop Clients can operate in one of two modes for call control:

- Softphone Mode — Using audio and video on a computer

  When a Jabber Desktop Client is in softphone mode, it is directly registered to Unified CM as a SIP endpoint for audio and video call control functionality, and it is configured on Unified CM as device type Client Services Framework.

- Deskphone Control Mode — Using a Cisco IP Phone for audio (and video, if supported)

  When a Jabber Desktop Client is in deskphone control mode, it does not register with Unified CM using SIP, but instead it uses CTI/JTAPI to initiate, monitor, and terminate calls, monitor line state, and provide call history, while controlling a Cisco Unified IP Phone. The Cisco CallManager Cisco IP Phone (CCMCIP) or UDS service on Unified CM is used by the Jabber Desktop Client to retrieve a list of devices associated with each user. This list of devices is used by a client in deskphone mode to choose which Cisco IP Phone it wishes to control.

Softphone Mode

When operating in softphone mode, the Jabber Desktop Client is a SIP line-side registered device on Unified CM, utilizing all the call control capabilities and functionality of a Cisco Unified IP Phone, including configuration of registration, redundancy, regions, locations, dial plan management, authentication, encryption, user association, and so forth. The Jabber Desktop Client supports a single line appearance for the user.

The SIP registered device of the Jabber Desktop Client must be factored in as a regular SIP endpoint, like any other SIP registered endpoint, for purposes of sizing calculations for a Unified CM cluster. The Jabber Desktop Client in softphone mode uses the CCMCIP or UDS service to discover its device name for registration with Unified CM.

Deskphone Control Mode

When operating in deskphone control mode, the Jabber Desktop Client uses CTI/JTAPI to provide the ability to place, monitor, and receive calls using Cisco Unified IP Phones. When audio calls are received or placed in this mode, the audio path is through the Cisco Unified IP Phone. For video calls, the video stream can originate and terminate either on the Cisco IP Phone (if it has a camera) or on the computer using a approved camera. The Jabber Desktop Client uses the CCMCIP or UDS service on Unified CM to discover the associated devices of the user.

When using deskphone control mode for the Jabber Desktop Client, factor the CTI scaling numbers into the Unified CM deployment calculations. For additional information about capacity planning, see the chapter on Collaboration Solution Sizing Guidance, page 25-1.

Jabber Desktop Clients – Audio, Video, and Web Conferencing Services

Access to scheduled conferencing services for clients can be provided through an HTTP interface. Cisco audio, video and web-based scheduled conferencing services can be provided by using the cloud-based WebEx Meeting Center service or a combination of on-premises WebEx Meeting Server for audio and video conferencing services and WebEx cloud-based web conferencing services. For more information about WebEx Meeting Center, refer to the documentation available at:

https://www.cisco.com/c/en/us/products/conferencing/webex-meeting-center/index.html

Jabber Desktop Clients – Contact Management

The Jabber Desktop Client can use one of the following contact sources for contact search and information:

- Cisco Unified CM User database via the User Data Service (UDS)
- LDAP directory integration
- WebEx Messenger service

Contacts can also be stored and retrieved locally using either of the following:

- Jabber Desktop Client Cache
- Local address books and contact lists such as Microsoft Outlook

The Jabber Desktop Client uses reverse number lookup to map an incoming telephone number to a contact, in addition to photo retrieval. The Jabber Desktop Client contact management allows for up to five search bases to be defined for LDAP queries.

Cisco Unified CM User Data Service (UDS)

UDS provides clients with a contact search service on Cisco Unified Communications Manager. You can synchronize contact data into the Cisco Unified CM User database from Microsoft Active Directory or other LDAP directory sources. Clients can then automatically retrieve that contact data directly from Unified CM using the UDS REST interface.

The UDS-to-LDAP Proxy feature is available as an alternate to sourcing contact information from the local Unified CM user database. With UDS-to-LDAP Proxy, contact searches are still handled by UDS but are proxied to the corporate LDAP directory, with UDS relaying results back to the Jabber client. This enables Jabber clients to search a corporate directory that exceeds the maximum number of users supported within the Unified CM database.

LDAP Directory

You can configure a corporate LDAP directory to satisfy a number of different requirements, including the following:

- User provisioning — You can provision users automatically from the LDAP directory into the Cisco Unified Communications Manager database using directory integration. Cisco Unified CM synchronizes with the LDAP directory content so that you avoid having to add, remove, or modify user information manually each time a change occurs in the LDAP directory.
- User authentication — You can authenticate users using the LDAP directory credentials. Cisco IM and Presence synchronizes all the user information from Cisco Unified Communications Manager to provide authentication for client users.
- User lookup — You can enable LDAP directory lookups to allow Cisco clients or third-party XMPP clients to search for contacts in the LDAP directory.

WebEx Directory Integration

Use the WebEx Administration Tool to implement WebEx Directory Integration. WebEx imports a comma-separated value (CSV) file of your enterprise directory information into its WebEx Messenger service. For more information, refer to the latest version of the *Cisco WebEx Messenger Administration Guide*, available at

https://www.cisco.com/c/en/us/support/unified-communications/webex-messenger/products-installation-guides-list.html

Jabber Desktop Client Cache

The Jabber Desktop Client maintains a local cache of contact information derived from previous directory queries and contacts already listed, as well as the local address book or contact list. If a contact for a call already exists in the cache, the Jabber Desktop Client does not search the directory. If a contact does not exist in the cache, the Jabber Desktop Client performs a directory search.

Directory Search

When a contact cannot be found in the local Jabber Desktop Client cache or contact list, a search for contacts can be made. The WebEx Messenger user can utilize a predictive search whereby the cache, contact list, and local Outlook contact list are queried as the contact name is being entered. If no matches are found, the search continues to query the corporate directory (WebEx Messenger database).

For more information about Cisco Jabber for Windows, refer to the data sheets and product documentation at

https://www.cisco.com/c/en/us/products/unified-communications/jabber-windows/index.html

For more information about the Cisco Jabber for Mac, refer to the data sheets and product documentation at

https://www.cisco.com/c/en/us/products/unified-communications/jabber-mac/index.html

Cisco Spark Desktop Clients

Cisco Spark desktop clients enable persistent cloud-based virtual team spaces that facilitate 1-to-1 and team collaboration. The Cisco Spark desktop client runs on Windows and Mac computers. Cisco Spark allows desktop application users to access collaboration services from the Cisco Collaboration Cloud, including secure and encrypted persistent messaging, voice and video calls over IP, and file sharing, all within virtual one-on-one or group collaboration spaces. The client communicates with the Cisco Collaboration Cloud using HTTPS for messaging and file sharing, while voice and video over IP media uses SRTP.

For proper Cisco Spark client operation, the desktop computer must be able to reach the Internet by connecting to a wired or wireless network (802.11 WLAN or mobile provider data network).

For more information about the Cisco Spark desktop clients, additional feature details, and supported hardware and software versions, refer to the Cisco Spark documentation at

https://support.ciscospark.com/

Cisco UC Integration™ for Microsoft Lync

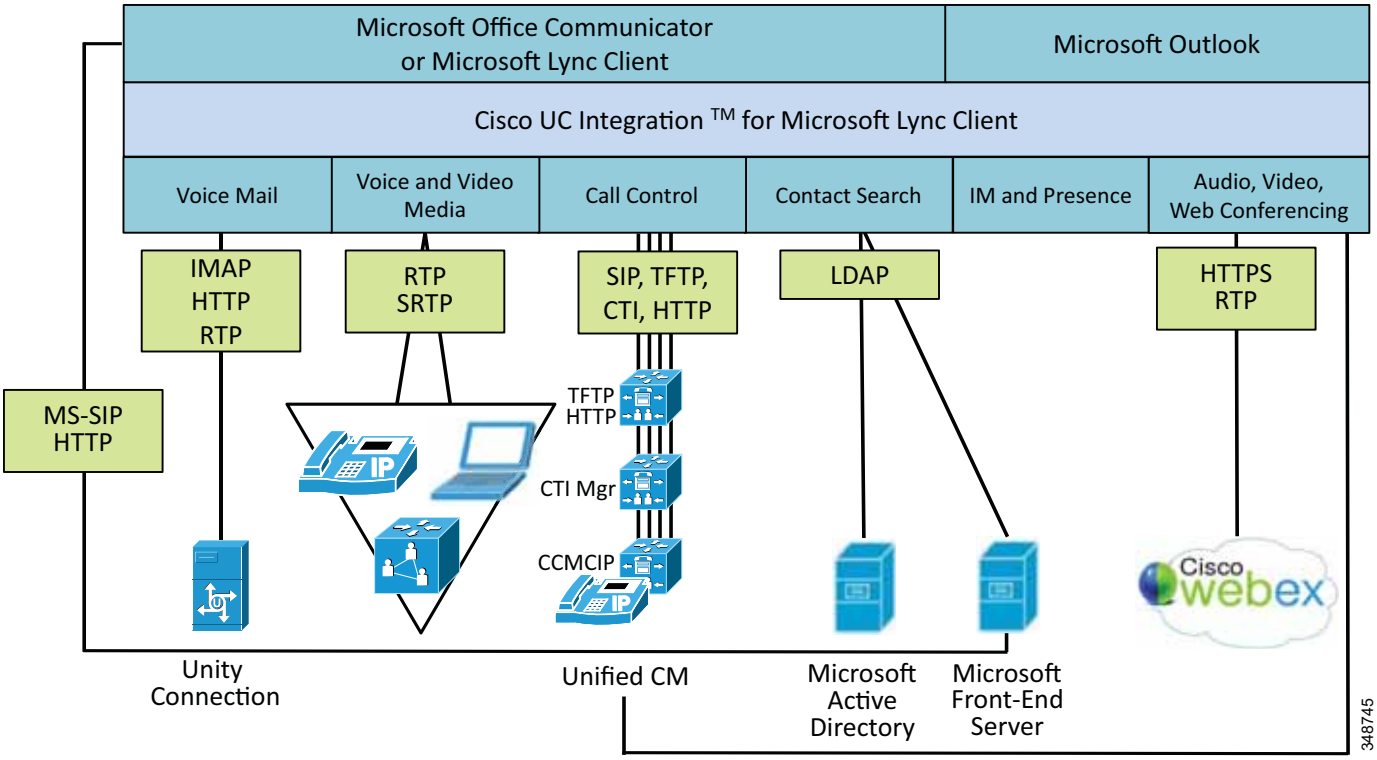
Cisco UC Integration™ for Microsoft Lync clients support a variation of the on-premises deployment models, where IM and presence services are provided by Microsoft Applications instead of Cisco IM and Presence.

Cisco UC Integration™ for Microsoft Lync allows for tightly integrated Cisco Unified Communications services for Microsoft Lync by integrating with underlying Unified Communications services. The solution extends the presence and instant messaging capabilities of Microsoft Lync by providing access to a broad set of Cisco Unified Communications services, including standards-based audio and video, unified messaging, web conferencing, deskphone control, and telephony presence, while delivering a consistent user experience.

Cisco UC Integration™ for Microsoft Lync Architecture

The solution architecture for a Cisco UC Integration™ for Microsoft Lync deployment, shown in Figure 8-3, includes Cisco Unified Communications Manager for audio and video services, Microsoft Office Communications Server 2007 for presence and instant messaging services, Microsoft Active Directory for user account information, Cisco Unified Communications services for PC audio or deskphone control, and Microsoft Lync.

Figure 8-3 Cisco UC Integration™ for Microsoft Lync Architecture



With a deployment of Cisco UC Integration™ for Microsoft Lync, the client utilizes user information from the Office Communications Server Address Book that gets downloaded to the client. The address book is generated and delivered to the clients from the Office Communications Server once the user is enabled for presence and instant messaging. Cisco recommends that administrators populate the user directory number information with an E.164 value (for example, +18005551212) and enable LDAP synchronization and authentication on Unified CM for user account consistency. Cisco UC Integration™ for Microsoft Lync connects to both Cisco Unified CM and Microsoft Active Directory and provides for account credential synchronization rules.

Note With Cisco UC Integration™ for Microsoft Lync, instant messaging and presence services are provided by Microsoft rather than by Cisco Unified Communications services.

Deploying and Configuring Cisco UC Integration™ for Microsoft Lync

When deploying Cisco UC Integration™ for Microsoft Lync, Cisco Unified Communications Manager provides the call control while Microsoft Lync provides the instant messaging and presence.

Cisco UC Integration™ for Microsoft Lync reads its configuration settings from a series of registry entries that the administrator must configure. Cisco recommends pushing these registry configuration settings from Microsoft Active Directory by means of Group Policy to distribute the configuration settings automatically to the client computer. Although Group Policy is the recommended installation mechanism, there are other methods available as well, including third-party software deployment tools, batch files, Vbscript, or manual configuration.

Microsoft Active Directory group policies can be extended using administration templates, and Cisco UC Integration™ for Microsoft Lync provides a template that the administrator can add to provide the group policy support. After the administrative template is loaded, a Cisco UC Integration™ for Microsoft Lync configuration policy can be created by the administrator for the registry configuration settings (TFTP servers, CTI servers, CCMCIP servers, voicemail, and LDAP servers).

The Group Policy Management Console can be used to control how and where these group policies are applied to different organizational units. From a client policy perspective, when you deploy Cisco UC Integration™ for Microsoft Lync, Cisco recommends setting the Microsoft Telephony Mode Policy to **IM and Presence Only** and **DisableAVConferencing**. These client policy changes will allow for only a single set of call options to be displayed in the Microsoft Lync user experience.

A Cisco UC Integration™ for Microsoft Lync deployment also allows for custom presence states to be defined and deployed in the cisco-presence-states-config.xml file that gets installed. However, Cisco recommends that administrators relocate this file to an HTTPs location, such as the Microsoft Office Communications Server, to allow Microsoft Lync to use this custom presence state file based on the following registry location:

HKLM\Software\Policies\Microsoft\Communicator\CustomStateURL

General Deployment Considerations for Software-Based Endpoints

The following sections list important design considerations for deploying software-based endpoints.

Quality of Service

Cisco software-based client applications do mark their traffic at Layer 3 in accordance with QoS marking best practices; however, even when the applications do mark traffic properly, the underlying operating system or hardware might not honor the markings. Given the general unpredictability and unreliability of traffic marking coming from desktop computers, as a general rule these traffic markings should not be trusted. This means that all traffic flows must be re-marked by the network based on protocol and/or port numbers, with real-time traffic flows being marked based on best practices. This includes re-marking of voice-only call media with DSC 46 or PHB EF, video call media (including voice) with DSCP 34 or PHB AF41, and call signaling with DSCP 24 or PHB CS3. These markings along with a properly configured network infrastructure ensure priority treatment for voice-only call media and dedicated bandwidth for video call media and call signaling. In addition to re-marking of software-based endpoint traffic, Cisco recommends using network-based policing and rate limiting to ensure that the software-based endpoint does not consume too much network bandwidth. This can occur when the desktop computer generates too much data traffic or when the endpoint application misbehaves and generates more voice and/or video media and signaling traffic than would be expected for a typical call. In cases where third-party software is used to fully control desktop computer network traffic

marking, administrators may decide to trust desktop computer marking, in which case re-marking of packets would not be required. Network-based policing and rate limiting is still recommended to protect the overall network in case of a misbehaving endpoint.

In the case of software-based Cisco IP Communicator and Cisco Jabber for Windows, appropriate Layer 3 DSCP QoS marking can be applied to audio and video streams based on voice and video media source port numbers using Microsoft Windows group policies.

For more information about Cisco Jabber for Windows QoS with Microsoft Windows group policies, refer to the Quality of Service configuration information in the latest version of *On-Premises Deployment for Cisco Jabber*, available at

https://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html

Inter-VLAN Routing

Because software-based endpoints run on a desktop computer usually deployed on a data VLAN, when software-based endpoints are deployed on networks with voice and data VLAN separation, inter-VLAN routing should be configured and allowed so that voice traffic from these endpoints on the data VLAN can reach endpoints on the voice VLAN.

SRST and Enhanced SRST

When deploying Cisco software-based endpoint desktop applications in branch locations separated from a centralized call processing platform by a low-speed or unreliable WAN link, it is important to consider local call processing redundancy. By using SRST or Enhanced SRST on a Cisco IOS router in each branch location, basic IP telephony services can be maintained for software-based endpoints when connectivity to the centralized call processing platform is lost. However, the set of available user-facing features is much smaller when a desktop software-based endpoint is registered to SRST than when the application is registered to Unified CM.

Secure Remote Enterprise Attachment

Cisco software-based endpoints can be securely connected to the enterprise network from remote locations using VPN or VPN-less solutions.

In the case of VPN-based connectivity, software-based endpoints can be located behind a VPN router that creates a secure VPN tunnel to the Cisco Adaptive Security Appliance (ASA) or other VPN head-end concentrator at the enterprise edge. This remote secure connectivity secures not only voice and video media and signaling traffic, but also all traffic coming from the personal computer. As a result, all traffic from the computer traverses the enterprise network edge even if that traffic is ultimately destined for the Internet.

Alternatively, Cisco Jabber desktop clients are able to leverage mobile and remote access functionality of the Cisco Expressway solution. This firewall traversal solution relies on TLS reverse proxy connectivity to the enterprise, as provided by the Cisco Expressway-E and Expressway-C servers for registration to Unified CM call control for voice and video calling and access to enterprise collaboration applications and services such as IM and presence, voicemail, and directory access. For more information about mobile and remote access capabilities of the Cisco Expressway solution, refer to the solution information and product documentation available at

https://www.cisco.com/c/en/us/products/unified-communications/expressway-series/index.html

Dial Plan

Dial plan and number normalization considerations must be taken into account when deploying software-based endpoints. Jabber desktop clients typically use the directory for searching, resolving, and adding contacts. The number that is associated with those contacts must be in a form that the client can recognize, resolve, and dial.

Deployments may vary, depending on the configuration of the directory and Unified CM. In cases where the directory contains E.164 numbering (for example, +18005551212) for business, mobile, and home telephone numbers and Unified CM also contains an E.164 dial plan, the need for additional dial rules is minimized because every lookup, resolution, and dialed event results in an E.164 formatted dial string.

If a Unified CM deployment has implemented a private dial plan (for example, 5551212), then translation of the E.164 number to a private directory number needs to occur on Unified CM. Outbound calls can be translated by Unified CM translation patterns that allow the number being dialed (for example, +18005551212) to be presented to the endpoint as the private number (5551212 in this example). Inbound calls can be translated by means of directory lookup rules. This allows an incoming number of 5551212 to be presented for reverse number lookup caller identification as +18005551212.

Private numbering plan deployments may arise, where the dial plan used for your company and the telephone number information stored in the LDAP directory may require the configuration of translation patterns and directory lookup rules in Cisco Unified Communications Manager to manage number format differences. Directory lookup rules define how to reformat the inbound call ID to be used as a directory lookup key. Translation patterns define how to transform a phone number retrieved from the LDAP directory for outbound dialing.

Translation patterns are used by Unified CM to manipulate the dialed digits before a call is routed, and they are handled strictly by Unified CM. Translation patterns are the recommended method for manipulating dialed numbers. For additional guidelines on translation pattern usage and dial plan management, see the chapter on Dial Plan, page 14-1.

Application dialing rules can be used as an alternative to translation patterns to manipulate numbers that are dialed. Application dialing rules can automatically strip numbers from, or add numbers to, phone numbers that the user dials. Application Dial Rules are configured in Unified CM and are downloaded to the client from Unified CM. Translation patterns are the recommended method for manipulating dialed numbers.

Directory lookup rules transform caller identification numbers into numbers that can be looked up in the directory. A directory lookup rule specifies which numbers to transform based on the initial digits and the length of the number. Directory lookup rules are configured in Unified CM and are downloaded to the client from Unified CM.

Before a call is placed through contact information, the client application removes everything from the phone number to be dialed, except for letters and digits. The application transforms the letters to digits and applies the dialing rules. The letter-to-digit mapping is locale-specific and corresponds to the letters found on a standard telephone keypad for that locale. For example, for a US English locale, 1-800-4UCSRND transforms to 18004827763. Users cannot view or modify the client transformed numbers before the application places the call.

Contact Sources

Cisco Jabber for Windows and Cisco Jabber for Mac default to using Cisco Directory Integration (CDI), which uses service discovery to automatically connect and authenticate to LDAP v3 compatible directories, including Microsoft Active Directory.

For integration with an LDAP directory that requires custom attribute mapping, these attribute mappings can be created in a configuration file that can be downloaded to the client from the Unified CM server.

Cisco Jabber desktop clients also support the Unified CM User Data Service (UDS), which allows a client to search for contacts using the Unified CM user database (which may be synchronized with an LDAP directory). UDS is used automatically by Jabber desktop clients for contact resolution when they are located outside of the corporate firewall and connected via Expressway mobile and remote access.

In addition, Jabber for Windows supports Microsoft Outlook local contact, which allows users to search for contacts that are in the user's Microsoft Outlook client.

Extend and Connect

Cisco Jabber desktop clients support Extend and Connect, which enables users to make and receive calls from Jabber using third-party phones. This allows users to utilize their existing third-party PBX phones while taking advantage of Cisco Collaboration features. There are several modes within Extend and Connect, and each mode requires different trunk usage. The dial plan must be designed carefully for Extend and Connect. For more details on dial plan design, see the chapter on Dial Plan, page 14-1. Extend and Connect is not supported when Jabber clients are outside the corporate network and connected through Expressway mobile and remote access.

OAuth with Refresh Login Flow

Beginning with Cisco Jabber 11.9, client authorization and authentication is facilitated using the OAuth 2.0 authorization framework. This provides for faster login and faster re-authentication during launch and network transitions. Prior to Cisco Unified CM 12.0 and Unified CM 11.5(1) SU3, Cisco Jabber used OAuth only when Single-Sign On (SSO) was enabled within the deployment. The OAuth implementation relies on the Unified CM publisher acting as an authorization server responsible for authenticating and then issuing authorization tokens to clients. This token, along with a refresh token, enables the client to request and gain authorization to collaboration services and to quickly renew an expired authorization token using the refresh token. For additional details on the OAuth 2.0 framework, refer to the section on Authorization Framework, page 16-45.

To leverage OAuth for Jabber client authorization and authentication, the **OAuth with Refresh Login Flow** service parameter must be enabled on Cisco Unified CM, Unified CM IM and Presence, and Unity Connection. Likewise, the **Authorize by OAuth token with refresh** setting must be enabled on Expressway-C for Jabber clients to use OAuth over Expressway Mobile and Remote Access.

For more information on deploying OAuth with Cisco Jabber, refer to the latest version of the white paper on *Deploying OAuth with Cisco Collaboration Solution Release 12.0*, available at

https://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html

Wireless Endpoints

Cisco wireless endpoints rely on an 802.11 wireless LAN (WLAN) infrastructure for network connectivity and to provide IP telephony functionality and features. This type of endpoint is ideal for mobile users that move around within a single enterprise location or between enterprise locations or environments where traditional wired phones are undesirable or problematic. Cisco offers the following voice and video over WLAN (VVoWLAN) IP phones:

- Cisco Unified Wireless IP Phones, including the Cisco Unified Wireless IP Phone 8821, 7925G, 7925G-EX, and 7926G
- Cisco IP Phone 8861 and 8865
- Cisco DX Series

All are hardware-based phones with built-in radio antenna. The Cisco Unified Wireless IP Phones 7925G, 7925G-EX, and 7926G enable 802.11b, 802.11g, or 802.11a connectivity to the network. The Cisco Unified Wireless IP Phone 8821 and Cisco IP Phones 8861 and 8865 enable 802.11a, 802.11b, 802.11g, 802.11n, and 802.11ac wireless connectivity while the Cisco DX Series endpoints enable 802.11a, 802.11b, 802.11g, and 802.11n wireless connectivity. The Cisco Unified Wireless IP Phones 7925G, 7925G-EX, and 7926G register and communicate with Cisco call processing platforms using SCCP signaling protocol. The Cisco Unified Wireless IP Phone 8821, Cisco IP Phones 8861 and 8865, and DX Series endpoints use the SIP signaling protocol to register and communicate with Cisco call processing platforms.

For more information about the Cisco Unified Wireless IP Phones, refer to the data sheets and product documentation available at

https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-7900-series/index.html

For more information about the Cisco IP Phone 8800 Series, refer to the data sheets and product documentation available at

https://www.cisco.com/c/en/us/products/collaboration-endpoints/unified-ip-phone-8800-series/index.html

For more information about the Cisco DX Series endpoints, refer to the data sheets and product documentation available at

https://www.cisco.com/c/en/us/products/collaboration-endpoints/desktop-collaboration-experience-dx600-series/index.html

General Deployment Considerations for Wireless Endpoints

The following sections list important design considerations for deploying wireless endpoints.

Network Radio Frequency Design and Site Survey

Before deploying wireless endpoints, you must ensure your WLAN radio frequency (RF) design minimizes same-channel interference while also providing sufficient radio signal levels and non-adjacent channel overlap so that acceptable voice and video quality can be maintained as the device moves from one location to another. In addition, you must perform a complete WLAN site survey to verify network RF design and to ensure that appropriate data rates and security mechanisms are in place. Your site survey should take into consideration which types of antennas will provide the best coverage, as well as where sources of RF interference might exist. Even when using third-party site survey tools,

Cisco highly recommends that you verify the site survey using the wireless endpoint device itself because each endpoint or client radio can behave differently depending on antenna sensitivity and survey application limitations. Cisco recommends relying on the 5 GHz WLAN band (802.11a/n) whenever possible for connecting wireless endpoints capable of generating voice and video traffic. 5 GHz WLANs provide better throughput and less interference for voice and video calls. Refer to the section on Wireless LAN Infrastructure, page 3-61, for more information about wireless network design.

Security: Authentication and Encryption

When deploying wireless endpoints, it is important to consider the security mechanisms used to control access to the network and to protect the network traffic. Cisco wireless endpoints support a wide range of authentication and encryption protocols including WPA, WPA2, EAP-FAST, PEAP, and so forth. Choose an authentication and encryption method that is supported by the WLAN infrastructure and the endpoint devices you deploy, and one that aligns with IT security policies. In addition, ensure that the authentication and encryption method chosen supports a fast rekeying method such as Cisco Centralized Key Management (CCKM) so that active voice and video calls can be maintained when the device is roaming from one location in the network to another.

Note In dual-band WLANs (those with both 2.4 GHz and 5 GHz bands), it is possible to roam between 802.11b/g and 802.11a with the same SSID, provided the client is capable of supporting both bands. However, with some devices this can cause gaps in the voice or video path. In order to avoid these gaps, use only one band for voice and video communications.

Wireless Call Capacity

When deploying wireless devices and enabling wireless device roaming within the enterprise WLAN, it is also important to consider the device connectivity and call capacity of the WLAN infrastructure. Oversubscription of the WLAN infrastructure in terms of number of devices or number of active calls will result in dropped wireless connections, poor voice and video quality, and delayed or failed call setup. The chances of oversubscribing a deployment of voice and video over WLAN are greatly minimized by deploying sufficient numbers of WLAN access points (APs) to handle required call capacities. AP call capacities are based on the number of simultaneous bidirectional streams that can be supported in a single channel cell area. The general rule for VVoWLAN call capacities is as follows:

- Maximum of 27 simultaneous VoWLAN bidirectional streams per 802.11g/n (2.4 GHz) channel cell with Bluetooth disabled or per 802.11a/n/ac (5 GHz) channel and 24 Mbps or higher data rates enabled.
- Maximum of 8 simultaneous VVoWLAN bidirectional streams per 802.11 g/n (2.4 GHz) channel cell with Bluetooth disabled or per 802.11 a/n/ac (5 GHz) channel cell assuming a video resolution of 720p (high-definition) and video bit rate of up to 1 Mbps.

These call capacity values are highly dependent upon the RF environment, the wireless handset features, and underlying WLAN system features. Actual capacities for a particular deployment could be less.

Note A single call between two wireless endpoints associated to the same AP is considered to be two simultaneous bidirectional streams.

The above capacities are based on voice activity detection (VAD) being disabled and a packetization sample size of 20 milliseconds (ms). VAD is a mechanism for conserving bandwidth by not sending RTP packets while no speech is occurring during the call. However, enabling or disabling VAD, also referred

to as Silence Suppression, is sometimes a global configuration depending on the Cisco call control platforms. Thus, if VAD is enabled for wirelessly attached Cisco Unified IP Phones, then it may be enabled for all devices in the deployment. Cisco recommends leaving VAD (Silence Suppression) disabled to provide better overall voice quality.

At a sampling rate of 20 ms, a voice call will generate 50 packets per second (pps) in either direction. Cisco recommends setting the sample rate to 20 ms for almost all cases. By using a larger sample size (for example, 30 or 40 ms), you can increase the number of simultaneous calls per AP, but a larger end-to-end delay will result. In addition, the percentage of acceptable voice packet loss within a wireless environment decreases dramatically with a larger sample size because more of the conversation is missing when a packet is lost. For more information about voice sampling size, see the section on Bandwidth Provisioning, page 3-52.

Bluetooth Support

The Cisco Unified Wireless IP Phones 8821, 7925G, 7925G-EX, and 7926G, the Cisco IP Phones 8861 and 8865, and the Cisco DX Series endpoints are Bluetooth-enabled devices. The Bluetooth radio or module within these wireless Cisco IP phones enables support for Bluetooth headsets. In addition, as previously mentioned, the Cisco IP Phones 8845, 8851, 8861, 8865, and DX Series endpoints support Intelligent Proximity for Mobile Voice with Bluetooth pairing for hands-free audio and mobile contact and call history sharing. Because Bluetooth devices use the same 2.4 GHz radio band as 802.11b/g devices, it is possible that Bluetooth and 802.11b/g-capable devices can interfere with each other, thus resulting in connectivity issues.

While the Bluetooth and 802.11 WLAN radios coexist natively in the Cisco Unified Wireless IP Phones, Cisco IP Phones 8861, 8865, and Cisco DX Series endpoints, greatly reducing and avoiding radio interference between the Bluetooth and 802.11b/g radio, the Bluetooth radio in these wirelessly attached phones can cause interference for other 802.11b/g and Bluetooth radio devices deployed in close proximity. Due to the potential for interference and disruption of 802.11b/g WLAN voice and video devices (which can result in poor voice and video quality, de-registration, and/or call setup delays), Cisco recommends deploying all WLAN voice and video devices on 802.11a, 802.11n, or 802.11ac, which use the 5 GHz radio band. By deploying wireless phones on the 5 GHz radio band, you can avoid interference caused by Bluetooth devices.

If deploying 802.11 WLAN devices on the 5 GHz radio band is not an option and interference on the 2.4 GHz radio band is causing connectivity, functionality, or voice and video quality issues, consider prohibiting or restricting the use of Bluetooth headsets and Bluetooth dependent features such as Intelligent Proximity for Mobile Voice within these deployments.

For more information on Intelligent Proximity for Mobile Voice and Bluetooth pairing on the Cisco 8851, 8861, and DX Series endpoints, see Intelligent Proximity, page 8-13.

Note Using Bluetooth wireless headsets with the battery-powered Cisco Unified Wireless IP Phones will increase battery power consumption on your phone and will result in reduced battery life.

Note The use of Bluetooth headsets and Bluetooth features such as Intelligent Proximity for Mobile Voice can cause interference and possibly service disruption for adjacent wireless clients and endpoints relying on the 2.4 GHz band (802.11b/g/n).

Quality of Service

When configuring network-level quality of service (QoS), Cisco wireless endpoints (including Cisco Unified Wireless IP Phones, the Cisco IP Phone 8861, and Cisco DX Series endpoints) can be trusted and their packet markings honored. By default these endpoints mark the recommended and appropriate Layer 3 values for voice and video media and call signaling (voice media as DSCP 46 or PHB EF; voice and video media as DSCP 34 or PHB AF41 for a video call, and call signaling as DSCP 24 or PHB CS3). Likewise, these devices mark appropriately at Layer 2 (voice media WMM User Priority (UP) of 6; voice and video media for video call WMM UP 5; call signaling WMM UP 4). With these packet markings, end-to-end voice quality on the converged network will be acceptable.

Despite appropriate packet marking at both Layer 2 and Layer 3, multipurpose devices such as the Cisco DX80 are capable of generating large amounts of non-real-time traffic. As such, concerns are sometimes raised regarding commingling of these devices on the same WLAN SSID or VLAN. While Layer 2 QoS marking and 802.11e WMM work to ensure that more bandwidth and more frequent access to the wireless medium are provided for real-time traffic, in dense or heavily utilized deployments, separating multi-purpose devices such as DX Series endpoints into a separate SSID may provide some relief. However, this separate SSID for multipurpose devices should still be configured with a Platinum QoS profile to ensure that real-time traffic generated by these devices is still given priority treatment across the wireless infrastructure.

SRST and Enhanced SRST

When deploying wireless endpoints in branch locations separated from a centralized call processing platform by a low-speed or unreliable WAN link, it is important to consider local call processing redundancy. By deploying SRST or Enhanced SRST on a Cisco IOS router in each branch location, basic IP telephony services can be maintained for wireless endpoints when connectivity to the centralized call processing platform is lost. However, the set of available user-facing features is much smaller when a wireless endpoint is registered to SRST than when it is registered to Unified CM.

Device Mobility

When wireless endpoints move between locations in a multi-site centralized call processing deployment, the Cisco Unified CM Device Mobility feature may be used to dynamically update the location of the device based on the IP address the device uses to register to Unified CM. This prevents issues with call routing, PSTN egress, and codec and media resource selection typically encountered when devices move between locations. For more information on Device Mobility, see the section on Device Mobility, page 21-14.

For more information about deploying wireless IP endpoints such as the Cisco Unified Wireless IP Phone 7925G, refer to the deployment guides at

https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-7900-series/products-implementation-design-guides-list.html

For more information about deploying wireless Cisco 8800 Series endpoints, refer to the deployment guide at

https://www.cisco.com/c/en/us/support/collaboration-endpoints/unified-ip-phone-8800-series/products-implementation-design-guides-list.html

For more information about deploying the Cisco DX Series endpoints wirelessly, refer to the deployment guide at

https://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-implementation-design-guides-list.html

Mobile Endpoints

Cisco mobile endpoint devices and mobile endpoint client applications register and communicate with Unified CM for voice and video calling services. These devices and clients also enable additional features and services such as enterprise messaging, presence, and corporate directory integration by communicating with other back-end systems such as Cisco Unity Connection, Cisco IM and Presence, and LDAP directories. Cisco offers the following mobile endpoint devices and clients:

- Cisco Jabber for Android and Apple iOS, page 8-37
- Cisco Spark Mobile Clients, page 8-37
- Cisco WebEx Meetings, page 8-38, for Android, BlackBerry and Apple iOS devices
- Cisco AnyConnect Secure Mobility Client, page 8-38, for Android and Apple iOS devices

Cisco Jabber for Android and Apple iOS

The Cisco Jabber mobile clients for Android and Apple iOS devices including the iPhone and iPad enable smartphones and tablets to make and receive enterprise calls using voice and video over IP. The Cisco Jabber mobile client application running on the Android or Apple iOS device registers and communicates with Unified CM using the SIP signaling protocol. The Cisco Jabber mobile client also enables additional features such as corporate directory access, enterprise visual voicemail, XMPP-based enterprise instant messaging and presence, and secure remote attachment with Cisco Expressway mobile and remote access.

For more information about Cisco Jabber for Android, refer to the data sheet and product documentation at

https://www.cisco.com/c/en/us/products/unified-communications/jabber-android/index.html

For more information about Cisco Jabber for iPhone and iPad, refer to the data sheet and product documentation at

https://www.cisco.com/c/en/us/products/unified-communications/jabber-iphone-ipad/index.html

Cisco Spark Mobile Clients

Cisco Spark mobile clients enable persistent cloud-based virtual team spaces that facilitate 1-to-1 and team collaboration. Cisco Spark allows mobile application users to access collaboration services from the Cisco Collaboration Cloud. Cisco Spark for Android, iPad, and iPhone clients provide secure and encrypted persistent messaging, voice and video calls over IP, and file sharing, all within virtual one-on-one or group collaboration spaces. These clients communicate with the Cisco Collaboration Cloud using HTTPS for messaging and file sharing, and SRTP for voice and video over IP media traffic.

For proper Cisco Spark client operation, the mobile client device must be able to reach the Internet by connecting to an 802.11 wireless LAN or mobile provider data network.

For more information about the Cisco Spark mobile clients, additional feature details, and supported hardware and software versions, refer to the Cisco Spark documentation at

https://support.ciscospark.com/

Cisco WebEx Meetings

The Cisco WebEx Meetings mobile client runs on specific Android, Apple iOS, BlackBerry, and Windows Phone mobile smartphones and tablets. This client enables mobile endpoints to participate in Cisco WebEx Meetings with a similar experience as with desktop browser-based Cisco WebEx Meetings. This client enables active participation in Cisco WebEx voice and video conferencing, including the ability to view participant lists and shared content.

For more information about Cisco WebEx mobile clients, refer to the product information at

https://www.cisco.com/c/en/us/products/conferencing/webex-meetings/index.html

Cisco AnyConnect Secure Mobility Client

The Cisco AnyConnect Secure Mobility Client enables secure remote connectivity for Cisco Jabber mobile device clients, enabling persistent enterprise access over mobile data networks and non-enterprise WLANs. This client application provides SSL VPN connectivity for Apple iOS and Android mobile devices through the Cisco AnyConnect VPN solution available with the Cisco Adaptive Security Appliance (ASA) head-end.

For more information on secure remote VPN connectivity using Cisco AnyConnect, refer to the Cisco AnyConnect Secure Mobility Client documentation available at

https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/tsd-products-support-series-home.html

Deployment Considerations for Mobile Endpoints and Clients

The following sections list important design considerations for deploying mobile endpoints and clients.

WLAN Design

Because Cisco Jabber mobile clients are often attached to a WLAN, all of the previously mentioned WLAN deployment considerations apply to mobile clients and devices, including WLAN RF design and verification by site survey. In particular, Cisco recommends relying on the 5 GHz WLAN band (802.11a/n/ac) whenever possible for connecting wireless endpoints capable of generating voice and video traffic. 5 GHz WLANs provide better throughput and less interference for voice and video calls. If the 2.4 GHz band is used for mobile clients and devices, Bluetooth should be avoided. Likewise, the WLAN channel cell voice-only and video call capacity numbers covered in the section on Wireless Call Capacity, page 8-34, should be considered when deploying these clients and devices.

Secure Remote Enterprise Attachment

If appropriately deployed, Cisco mobile endpoints and clients can also connect to the enterprise from remote locations by using public or private 802.11 Wi-Fi hot spots or over the mobile data network. In these scenarios, mobile endpoints and clients can be securely connected using VPN or VPN-less solutions. In the case of VPN, the Cisco AnyConnect mobile VPN client can be used to connect the device or client to the enterprise with a secure SSL tunnel.

One important consideration for Cisco Jabber and Cisco AnyConnect deployments is the traffic being secured. When using the Cisco AnyConnect mobile VPN client on a mobile device with Cisco Jabber, the default behavior is that all traffic to and from the device is sent via the encrypted VPN tunnel and

into or through the enterprise. This might not be desirable in all deployments. In the case of Cisco Jabber, the preferred behavior may be to send only the Jabber-specific traffic through the enterprise via the VPN tunnel, while all other traffic is sent outside the tunnel. This can be accomplished by using the split-tunnel feature, which enables administrators to specify which traffic (based on destination subnets) traverses the VPN tunnel and which traffic goes in the clear. To secure just the Jabber traffic, administrators must configure for inclusion in the tunnel the IP subnets of the Cisco Unified Communications Manager cluster, IM and Presence cluster, voicemail server, directory server, and Trivial File Transfer Protocol (TFTP) server as well as the IP subnets for any endpoints they might connect with. Hence, the split-include policy should include the corporate network IP address range. Sometimes the IP space of a large company is not contiguous because of acquisitions and other events, so this configuration might not be applicable for all deployments.

For more information on Cisco Jabber and Cisco AnyConnect with split-tunnel includes, refer to the *Cisco AnyConnect Deployment Guide for Cisco Jabber*, available at

https://www.cisco.com/c/dam/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/guide_c07-717020.pdf

For VPN-less connectivity, Cisco Jabber mobile clients are able to leverage mobile and remote access functionality of the Cisco Expressway solution. This firewall traversal solution relies on TLS reverse proxy connectivity to the enterprise, as provided by the Cisco Expressway-E and Expressway-C servers for registration to Unified CM call control for voice and video calling and access to enterprise collaboration applications and services such as IM and presence, voicemail, and directory access. For additional information about mobile and remote access capabilities of the Cisco Expressway solution, refer to the solution information and product documentation available at

https://www.cisco.com/c/en/us/products/unified-communications/expressway-series/index.html

Quality of Service

Cisco mobile client applications and devices generally mark Layer 3 QoS packet values in accordance with Cisco collaboration QoS marking recommendations. This includes marking voice-only call media traffic with DSCP 46 or PHB EF, video call media (including voice) traffic with DSCP 34 or PHB AF41, and call signaling traffic with DSCP 24 or PHB CS3. Despite appropriate mobile client and device application Layer 3 packet marking, Layer 2 802.11 WLAN packet marking (User Priority, or UP) presents further challenges. Some devices may appropriately mark wireless Layer 2 802.11 User Priority (UP) values (voice-only call media UP 6, video call media UP 5, and call signaling UP 3). However, because Cisco mobile clients run on a variety of mobile devices, Layer 2 wireless QoS marking is inconsistent and therefore cannot be relied upon to provide appropriate treatment to traffic on the WLAN. In deployments with Cisco Unified Wireless LAN Controllers, enabling wireless SIP call admission control (CAC) might provide some relief for incorrect or nonexistent Layer 2 WLAN marking. SIP CAC utilizes media session snooping and ensures that downstream voice and video frames are prioritized and/or treated correctly. Even assuming appropriate mobile client application Layer 3 or even Layer 2 packet marking, mobile devices present many of the same challenges as desktop computers in terms of generating many different types of traffic, including both data and real-time traffic. Given this, mobile devices generally fall into the untrusted category of collaboration endpoints. For deployments where mobile client devices are not considered trusted endpoints, packet re-marking based on traffic type and port numbers is required to ensure that network priority queuing and dedicated bandwidth are applied to appropriate traffic. In addition to re-marking the mobile device traffic, Cisco recommends using network-based policing and rate limiting to ensure that the mobile client devices do not consume too much network bandwidth.

Note Mobile clients and devices may attach remotely to the enterprise using Cisco AnyConnect client over the mobile data network or public or private Wi-Fi hot spots. Because these connections traverse the Internet, there is no end-to-end QoS on the IP path and therefore all traffic is treated as best-effort. Voice and video quality cannot be guaranteed over these types of connections.

SRST and Enhanced SRST

When deploying mobile endpoints and clients such as Cisco Jabber for iPhone in branch locations separated from a centralized call processing platform by a low-speed or unreliable WAN link, it is important to consider local call processing redundancy. Cisco Jabber mobile clients do not support SRST; however, because most Cisco Jabber mobile clients run on smartphones with cellular voice radios, users may still be able to make call using the mobile provider network.

For additional design and deployment information about Cisco Jabber mobile clients, refer to the section on Cisco Mobile Clients and Devices, page 21-76.

Intelligent Proximity

As previously mentioned, Intelligent Proximity refers to features that leverage proximity-based connections between Cisco hardware endpoints and mobile devices.

Intelligent Proximity for Mobile Voice capabilities available on the Cisco 8851, 8861, and DX Series endpoints rely on Bluetooth pairing between the IP endpoint and a cellular or smart phone, enabling hands-free audio and mobile contact and call history sharing.

As indicated previously, Intelligent Proximity for Mobile Voice on the 8851, 8861, and DX Series endpoints and the Unified Mobility feature set are compatible. Further, Intelligent Proximity for Mobile Voice on the 8851 and 8861 IP Phones is also compatible with Cisco Jabber, enabling audio-playout on the IP Phone 8851 and 8861 while the video is played on the Jabber client device.

For more information on Intelligent Proximity and Bluetooth pairing, see Intelligent Proximity, page 8-13.

Contact Sources

Cisco Jabber for Android and iOS defaults to using Cisco Directory Integration (CDI), which relies on integration to LDAP v3 compatible directories, including Microsoft Active Directory.

For integration with an LDAP directory that requires custom attribute mapping, these attribute mappings can be created in a configuration file that can be downloaded to the client from the Unified CM server.

Cisco Jabber mobile clients also support the Unified CM User Data Service (UDS), which allows a client to search for contacts using the Unified CM user database (which may be synchronized with an LDAP directory). UDS is used automatically by Jabber mobile clients for contact resolution when they are located outside of the corporate firewall and connected via Expressway mobile and remote access.

The UDS-to-LDAP Proxy feature is available as an alternate to sourcing contact information from the local Unified CM user database. With UDS-to-LDAP Proxy, contact searches are still handled by UDS but are proxied to the corporate LDAP directory, with UDS relaying results back to the Jabber client. This enables Jabber clients to search a corporate directory that exceeds the maximum number of users supported within the Unified CM database.

OAuth with Refresh Login Flow

Beginning with Cisco Jabber 11.9, client authorization and authentication is facilitated using the OAuth 2.0 authorization framework. This provides for faster login and faster re-authentication during launch and network transitions. Prior to Cisco Unified CM 12.0 and Unified CM 11.5(1) SU3, Cisco Jabber used OAuth only when Single-Sign On (SSO) was enabled within the deployment. The OAuth implementation relies on the Unified CM publisher acting as an authorization server responsible for authenticating and then issuing authorization tokens to clients. This token, along with a refresh token, enables the client to request and gain authorization to collaboration services and to quickly renew an expired authorization token using the refresh token. For additional details on the OAuth 2.0 framework, refer to the section on Authorization Framework, page 16-45.

To leverage OAuth for Jabber client authorization and authentication, the **OAuth with Refresh Login Flow** service parameter must be enabled on Cisco Unified CM, Unified CM IM and Presence, and Unity Connection. Likewise, the **Authorize by OAuth token with refresh** setting must be enabled on Expressway-C for Jabber clients to use OAuth over Expressway Mobile and Remote Access.

For more information on deploying OAuth with Cisco Jabber, refer to the latest version of the white paper on *Deploying OAuth with Cisco Collaboration Solution Release 12.0*, available at

https://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html

Apple Push Notification Service (APNs)

Cisco Jabber for iPhone and iPad 11.9 and later provides support for Apple Push Notification service (APNs) for receiving incoming call and message notifications when the client is running in the background.

Previously, like other Jabber clients, the Jabber for Apple iOS client (iPhone and iPad) leveraged periodic direct IP socket keepalives to maintain connectivity for voice and video over IP (VVoIP) and IM and presence services when the client moved to the background. Because Apple is deprecating the direct IP socket method for notifications, APNs will soon be required for sending notifications to Jabber for iOS clients running in the background on the Apple iOS device.

Cisco Spark for Apple iOS also supports APNs for receiving incoming call and message notifications when the client is running in the background.

Note APNs has *no* impact on non-iOS Cisco Spark clients (Cisco Spark for Android, Cisco Spark for Windows, and Cisco Spark for Mac) and non-iOS Cisco Jabber clients (Jabber for Android, Jabber for Windows, and Jabber for Mac).

Refer to the section on Apple Push Notification Service (APNs) for Cisco Jabber for iPhone and iPad, page 21-99, for more information about APNs for Cisco Jabber clients.

Cisco Virtualization Experience Media Engine

The Cisco Virtualization Experience Media Engine (VXME) provides an integral collaboration software component by extending the Cisco Jabber collaboration experience to a Virtual Desktop Infrastructure (VDI) environment. VXME is a software package installed on a local platform (a thin client), and it allows users to enhance their VDI sessions to include locally terminated voice and video real-time communications, bypassing real-time media routing through the virtual desktop while allowing for a fully integrated user experience. The hosted virtual desktop is supported with Citrix XenDesktop, Citrix XenApp Published Desktop, or VMware View, through locally installed Citrix Receiver or VMware View Client, respectively. Regardless of the host VDI platform, a user has a consistent voice, video, and virtual desktop experience using Cisco Jabber on the virtual desktop with fully integrated accessories enabled for Unified Communications and seamless integration with VXME.

For more information on Cisco Virtualization Experience Media Engine (VXME), refer to the data sheet and product documentation at

https://www.cisco.com/c/en/us/products/collaboration-endpoints/virtualization-experience-media-engine/index.html

Deployment Considerations for Cisco Virtualization Experience Media Engine

The following sections list important design considerations for deploying Cisco Virtualization Experience Media Engine (VXME).

Quality of Service

No additional configuration is required for Cisco Virtualization Experience Media Engine (VXME) if the network is set up for 8021.q Dual VLAN. If the network is not setup for 802.1q Dual VLAN, QoS will be best-effort and the thin client should be placed in the data VLAN. For details on traffic marking, refer to the QoS design guides available at

https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-ipv6/design-guide-listing.html

Call admission control for voice and video follow existing Cisco Unified IP Phone guidelines, and bandwidth controls for the virtual desktop are provided through the connection broker settings.

SRST and Enhanced SRST

When deploying Cisco VXME in branch locations separated from a centralized call processing platform by a low-speed or unreliable WAN link, it is important to consider local call processing redundancy. If Jabber is running in deskphone control mode, during a WAN failure the hosted virtual desktop (HVD) where the Cisco Jabber client runs will continue to have contact with the Cisco Unified CM co-located in the data center. However, Cisco Unified CM connectivity to the desktop phone paired with the VXC zero client will be lost. By using Survivable Remote Site Telephony (SRST) or Enhanced SRST on a Cisco IOS router in each branch location, basic IP telephony services can be maintained for the desktop phones paired with the VXC clients to the centralized call processing platform is lost.

VXME does not support SRST or Enhanced SRST.

Third-Party IP Phones

Some third-party IP phones and devices may be integrated with Cisco call control to provide basic IP telephony functionality, as described in this section.

Third-Party SIP IP Phones

Third-party phones have specific local features that are independent of the call control signaling protocol, such as features access buttons (fixed or variable). Basic SIP RFC support allows for certain desktop features to be the same as on Cisco Unified IP Phones and also allows for interoperability of certain features. However, these third-party SIP phones do not provide the full feature functionality of Cisco Unified IP Phones.

Cisco works with key third-party vendors who are part of the Cisco Developer Network and who are developing solutions that leverage Cisco Unified CM and Unified CME SIP capabilities. For example, Tenacity Operating provides a software-based endpoint called accessaphone ipTTY, which enables terminal teletype (TTY) or text-based communications for IP telephony. This software-based endpoint can register and communicate with Cisco Unified CM as a third-party SIP phone.

For more information on Cisco's line-side SIP interoperability, refer to the Cisco Unified Communications Manager programming guides at

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-programming-reference-guides-list.html

For more information on the Cisco Developer Network and third-party development partners, refer to the information available on the Cisco Developer Community at

https://developer.cisco.com

High Availability for Collaboration Endpoints

To stay in service even during failure of the call control platform, Cisco endpoints are capable of being configured with multiple server nodes or servers for registration and call control service redundancy.

In the case of Cisco Unified CM call control, either through direct configuration or through DHCP during the boot-up phase, collaboration endpoints can accept and process more than one TFTP server address. In case the primary TFTP server is down when the endpoint boots up, the endpoint can get its configuration files from the secondary TFTP server.

Each of the endpoints is also associated with a device pool. The device pool contains a Unified CM Group that has one or more Unified CM subscribers. A list of these subscribers is sent to the endpoints in their configuration files. The endpoints attempt to register with the first (the primary) subscriber in the list. If that Unified CM subscriber is unavailable, the endpoint attempts to register with the second subscriber in the list (the secondary), and so on. Once registered to a subscriber, an endpoint can fail-over to another subscriber in the priority list in the Unified CM Group if the current subscriber fails. When a higher-priority subscriber comes back up, the endpoint will re-register to it.

In the case of those endpoints leveraging CTI, for example Cisco Jabber desktop client running in deskphone control mode, CTI service redundancy is required. In those cases, multiple Unified CM nodes should be running the Cisco CTIManager service so that Unified CM Group configuration will provide client failover from the primary to a secondary CTIManager node in the event of a node failure.

To protect against network failure for endpoints located across a WAN from the Unified CM cluster, a locally available Cisco Integrated Services Router (ISR) or other Cisco IOS router with SRST or Enhanced SRST may also be configured in the list of servers with which the endpoint may register. In case of a WAN failure, the endpoints register to the SRST router and provide uninterrupted voice

telephony services (although the set of features they support in SRST mode might be smaller). Note that some endpoints, including Cisco Jabber and Cisco TelePresence System video endpoints, do not support SRST.

Capacity Planning for Collaboration Endpoints

Cisco call control platforms support the following high-level endpoint capacities:

- A Cisco Unified CM cluster, even when deployed as part of Cisco Business Edition 7000, supports a maximum of 40,000 SCCP or SIP endpoints.
- When deployed as part of Cisco Business Edition 6000, a Cisco Unified CM cluster supports a maximum of 2,500 SCCP or SIP endpoints, depending on the server type.
- Cisco Business Edition 4000 supports a maximum of 200 SIP endpoints.
- Cisco Unified CM Express supports a maximum of 450 SCCP or SIP endpoints.
- Cisco Expressway-C and Expressway-E cluster pairs support a maximum of 10,000 remote endpoint proxy registrations.

The above numbers are nominal maximum capacities. The maximum number of endpoints that the call control platform will actually support depends on all of the other functions that the platform is performing, the busy hour call attempts (BHCA) of the users, and so forth, and the actual capacity could be less than the nominal maximum capacity. Unified CM CTI capacity must also be considered when sizing the system to ensure that Jabber desktop clients and other deskphone control applications have sufficient CTI capacity for operation. For more information on CTI sizing, refer to the chapter on Collaboration Solution Sizing Guidance, page 25-1.

In addition to call control platform capacity, network capacity must be considered with regard to bandwidth and call capacity. Of particular concern are 802.11 wireless attached devices such as the Cisco Unified Wireless IP Phone 7925G or an Android smartphone running Cisco Jabber, where network endpoint capacity is not determined by the number of physical ports but by the amount of bandwidth and throughput available on the shared wireless network. See Wireless Call Capacity, page 8-34, for voice and video call capacities per 802.11 channel cell.

For more information on endpoint capacity with Cisco call control, including platform-specific endpoint capacities per node, see the chapter on Collaboration Solution Sizing Guidance, page 25-1.

Design Considerations for Collaboration Endpoints

The following list summarizes high-level design recommendations for deploying Cisco endpoints:

- Analog gateways are available both as standalone devices and as integrated interface modules on Cisco IOS multiservice routers, and both types can be used within the same deployment. Select the analog gateway or gateways that meet analog port density requirements across company locations. Ensure that appropriate port capacity is provided for all locations in order to accommodate the required analog devices.
- Enable the role of **Standard CTI Allow Control of Phones supporting Connected Xfer and conf** for the end-user configuration associated with the device in order to enable CTI monitoring and control of Cisco IP Phone 8800 Series and Cisco DX Series endpoints. Only after this role has been enabled can CTI applications monitor or control these phones.

- To minimize endpoint firmware upgrade times over the WAN to remote branches, consider deploying a local TFTP server at the remote location and point endpoints located in that branch to this local TFTP server using the **load server** parameter. Alternatively, consider the use of the Peer File Sharing (PFS) feature when all or most of the devices at a particular remote location are the same phone model.
- Cisco Unified IP desk phones can be powered by power over Ethernet (PoE) when plugged into inline power-capable switches or when deployed with an inline power injector. Consider the use of inline power to reduce downtime and eliminate the need for an external power supply and wall power outlet.
- When deploying Cisco endpoints in branch locations separated from a centralized call processing platform by a low-speed or unreliable WAN link, it is important to consider local call processing redundancy. By using SRST or Enhanced SRST on a Cisco IOS router in each branch location, basic IP telephony services can be maintained for the desk phones when connectivity to the centralized call processing platform is lost. However, the set of available user-facing features is much smaller when a device is registered to SRST than when the phone is registered to Unified CM.
- For deployments with network voice and data VLAN separation, ensure that inter-VLAN routing has been configured and allowed so that Cisco software-based endpoints that run on desktop computers usually connected to data VLANs can communicate with endpoints on the voice VLAN. This is also important for endpoints on the voice VLAN that may be dependent on data VLAN-based resources that provide services such as directory and management.
- A WLAN site survey must be conducted to ensure appropriate RF design and to identify and eliminate sources of interference prior to deploying wireless and mobile endpoints capable of generating real-time traffic on the wireless network. This is necessary to ensure acceptable voice and video quality for calls traversing the WLAN.
- Select a WLAN authentication and encryption method that not only adheres to company security policies but also enables fast rekeying or authentication so that audio and video calls are not interrupted when wireless endpoints move from one location to another.
- Cisco recommends relying on the 5 GHz WLAN band (802.11a/n/ac) whenever possible for connecting wireless endpoints and mobile client devices capable of generating voice and/or video traffic. 5 GHz WLANs provide better throughput and less interference for voice and video calls. If the 2.4 GHz band is used for connecting wireless client devices and endpoints, Bluetooth should be avoided.
- Provide appropriate network and call control capacity to support the number of endpoints deployed. First, consider the endpoint registration and configuration capacities per call control platform: maximum of 40,000 endpoints per Unified CM cluster, even when deployed as part of Cisco Business Edition 7000; 2,500 endpoints per cluster when deployed as part of Cisco Business Edition 6000; 200 SIP endpoints when deployed on Cisco Business Edition 4000; or 10,000 remote endpoint registrations over Cisco Expressway. Next, consider call capacities per wireless channel cell for wireless attached endpoints, and the maximum of 27 bidirectional voice-only streams or maximum of 8 simultaneous voice and video streams or calls per WLAN channel cell.
- Ensure that the end-to-end network infrastructure has been configured with appropriate QoS policies, including marking and re-marking as appropriate, trust boundaries, queuing with both priority and dedicated bandwidth queues, rate limiting, and policing, so that collaboration endpoints deliver high-quality voice and video to end users.